Europeiska unionens
officiella tidning

SV
L-serien

2026/2394

6.11.2026

KOMMISSIONENS REKOMMENDATION (EU) 2026/2394

av den 29 oktober 2026

om icke-bindande standardavtalsvillkor för åtkomst till och användning av data och icke-bindande standardavtalsklausuler för molnavtal

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DENNA REKOMMENDATION

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 292,

med beaktande av Europaparlamentets och rådets förordning (EU) 2023/2854 av den 13 december 2023 om harmoniserade regler för skälig åtkomst till och användning av data och om ändring av förordning (EU) 2017/2394 och direktiv (EU) 2020/1828 ([1]) (*dataförordningen*), särskilt artikel 41, och

av följande skäl:

(1) Rättvisa avtalsenliga rättigheter och skyldigheter främjar förtroendet mellan marknadsaktörerna och kan bidra till ökad skälig åtkomst till och användning av data samt en mer konkurrenskraftig marknad för databehandlingstjänster, vilket gör det möjligt att fullt ut utnyttja fördelarna med en dataekonomi i unionen.

(2) För att tillgodose den digitala ekonomins behov och undanröja hinder för en väl fungerande inre marknad för data inrättades genom förordning (EU) 2023/2854 en harmoniserad ram som specificerar vem som har rätt att använda produktdata eller data från tillhörande tjänster samt villkoren och grunden för detta. Det centrala verktyg som förordning (EU) 2023/2854 använder för detta ändamål är avtal. Sedan den förordningen började tillämpas baseras användningen av data inte längre på en de facto kontroll över data, utan på avtal. Detta görs för att skapa rättssäkerhet när det gäller parternas rättigheter och skyldigheter och därmed främja datadelning. Dessutom syftar förordning (EU) 2023/2854 till att genom balanserade avtal säkerställa en rättvis fördelning av fördelarna för alla parter i datavärdekedjan.

(3) Förordning (EU) 2023/2854 fastställer rättigheter och skyldigheter för parter som är involverade i åtkomst till och användning av data, samt regler för obligatorisk datadelning, samtidigt som parterna genom avtal kan bestämma hur de praktiskt ska utöva sina rättigheter och skyldigheter i samband med sådan dataåtkomst och dataanvändning.

(4) Databehandlingstjänster är en grundläggande förutsättning för den digitala omställningen och en nyckelfaktor för konkurrenskraften i den digitala tidsåldern. Kundens möjlighet att byta från en tjänst till en annan eller att använda flera leverantörers tjänster samtidigt är en viktig förutsättning för en mer konkurrenskraftig marknad med lägre inträdeshinder för nya leverantörer. Förordning (EU) 2023/2854 fastställer regler om kundernas rätt att byta från en leverantör av databehandlingstjänster till en annan leverantör eller till lokal infrastruktur, och anger särskilda villkor och förfaranden, som även omfattar säkerhet och driftskontinuitet under bytet. Förordning (EU) 2023/2854 tar också hänsyn till parallell användning av flera databehandlingstjänster, vilket stöder en lyckad tillämpning av multimolnstrategier. Dessutom föreskriver förordning (EU) 2023/2854 att alla parter som är involverade i bytet måste samarbeta i god tro.

(5) Rättigheter och skyldigheter för kunder och leverantörer av databehandlingstjänster definieras i avtal om databehandlingstjänster. Genom förordning (EU) 2023/2854 införs en skyldighet för leverantörer av databehandlingstjänster att undanröja hinder som kan hindra kunder från att byta leverantör, inbegripet avtalsmässiga hinder.

(6) Enligt artikel 41 i förordning (EU) 2023/2854 har kommissionen till uppgift att utarbeta standardavtalsvillkor för åtkomst till och användning av data samt standardavtalsklausuler för molnavtal, som ett verktyg för att stödja parterna i förhandlingar och ingående av sådana avtal och för att främja mallar som innehåller rättvisa, rimliga och icke-diskriminerande avtalsenliga rättigheter och skyldigheter.

([1]) EUT L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj.

(7) Enligt förordning (EU) 2023/2854 är det primära syftet med dessa mallar att hjälpa företag, särskilt små och medelstora företag, att utarbeta, förhandla fram och ingå sådana avtal. I förordning (EU) 2023/2854 anges också att dessa standardavtalsvillkor, när de används brett och på ett integrerat sätt, bör ha den positiva effekten att de påverkar utformningen av avtal om åtkomst till och användning av data och därmed mer generellt leder till rättvisare avtalsförhållanden för åtkomst till och delning av data.

(8) Dessa syften visar att standardavtalsvillkor och standardavtalsklausuler bör spela en viktig roll vid tillämpningen av förordning (EU) 2023/2854 och för att visa hur balanserade avtal som tillämpar förordning (EU) 2023/2854 kan utformas, även för domstolar när de tillämpar den allmänna klausulen om skälighetsprövning som fastställs i förordning (EU) 2023/2854. Vidare bör tvistlösningsorganen, i enlighet med skäl 55 i förordning (EU) 2023/2854, beakta standardavtalsvillkoren för att säkerställa en enhetlig tillämpning av förordningen.

(9) Avtalsfrihet är ett grundläggande begrepp i förbindelser mellan företag och omfattas som sådant av näringsfriheten enligt Europeiska unionens stadga om de grundläggande rättigheterna. Kommissionen tillhandahåller härmed marknadsaktörerna mallar för deras avtalsförhållanden som inte är bindande och som, om avtalsparterna väljer att använda dem, kan anpassas. Detta förklaras också i bilaga I, där standardvillkoren och standardklausulerna beskrivs. Dessa villkor och klausuler har i första hand utarbetats för förbindelser mellan företag med beaktande av förordning (EU) 2023/2854 och annan unionslagstiftning. Som är fallet för alla avtal måste parterna, när de ingår avtalsförhållanden som rör data, följa tvingande bestämmelser i unionsrätten, såsom förordning (EU) 2023/2854, Europaparlamentet och rådets förordning (EU) 2016/679 ([2]) eller tvingande bestämmelser i konsumentlagstiftningen, samt tvingande bestämmelser i den nationella rätt som är tillämplig på det specifika avtalet.

(10) Oskäliga avtalsvillkor kan göra åtkomst till data eller byte av leverantörer av databehandlingstjänster affärsmässigt mindre lönsamt och ibland ekonomiskt oöverkomligt.

(11) Genom förordning (EU) 2023/2854 införs en skälighetsprövning av avtalsvillkor om åtkomst till och användning av data eller ansvar och rättsmedel vid överträdelse eller uppsägning av datarelaterade skyldigheter, när dessa ensidigt införts av en part i avtal som ingåtts mellan företag. I standardvillkoren och standardklausulerna beaktades också bestämmelserna om denna skälighetsprövning.

(12) Det är nödvändigt att fastställa standardavtalsvillkor för flera avtal som omfattar åtkomst till och användning av data inom ramen för kapitlen II, III och IV i förordning (EU) 2023/2854. Det första rekommenderade standardavtalet reglerar det rättsliga förhållandet mellan en användare av en uppkopplad produkt eller tillhörande tjänst, som enligt förordning (EU) 2023/2854 har rätt att få åtkomst till och använda data, och en datahållare (bilaga II). Dessa standardavtalsvillkor kan användas som ett separat avtal parallellt med andra avtal, nämligen a) avtalet om köp, hyra eller leasing av en uppkopplad produkt, b) avtalet om tillhandahållande av tillhörande tjänster eller c) alla avtal som är nödvändiga att ingå enligt förordning (EU) 2016/679. De kan dock också integreras i ett övergripande avtal, till exempel om köp av den uppkopplade produkten. Den andra typen av avtal som omfattas av standardavtalsvillkoren är mellan användaren och en datamottagare (bilaga III). Det tredje standardavtalet som omfattas är mellan datahållaren och en datamottagare, och gäller fall där en datahållare har en rättslig skyldighet att göra data tillgängliga för en tredje part, till exempel en skyldighet att göra data om uppkopplade produkter eller data från en tillhörande tjänst tillgängliga för en datamottagare som anges av användaren (bilaga IV). Det fjärde standardavtalet som omfattas ingås mellan företrädare som delar data på frivillig basis och är föremål för skälighetsprövning enligt förordning (EU) 2023/2854 (bilaga V).

(13) Det är nödvändigt att fastställa standardavtalsklausuler som kan införas i avtal om databehandlingstjänster för att återspegla kundernas och leverantörernas rättigheter och skyldigheter, mot bakgrund av kapitel VI i förordning (EU) 2023/2854 och med beaktande av nödvändigheten av att undanröja avtalsmässiga hinder för byte och säkerställa rättvisa, rimliga och icke-diskriminerande avtalsenliga rättigheter och skyldigheter (bilagorna VI–XII).

([2]) Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

(14) För att underlätta användningen av standardvillkoren och standardklausulerna bör vägledning och förklaringar i form av informationsrutor inkluderas. Vägledningen och förklaringarna är avsedda att stödja parterna genom att hänvisa till relevanta rättsliga skyldigheter, korshänvisa mellan villkoren och klausulerna och, när så är nödvändigt, förklara konsekvenserna av de val som parterna måste göra. Detta återspeglas i de olika alternativen för ett visst avtalsvillkor eller en viss avtalsklausul.

HÄRIGENOM REKOMMENDERAS FÖLJANDE.

(1) Att de avtalsslutande parterna använder de standardavtalsvillkor för åtkomst till och användning av data som anges i bilagorna I–V.

(2) Att de avtalsslutande parterna använder de standardavtalsklausuler som anges i bilagorna I och VI–XII för molnavtal.

(3) Att medlemsstaterna främjar användningen av de rekommenderade standardavtalsvillkoren och standardavtalsklausulerna, bland annat genom sina utsedda tvistlösningsorgan och behöriga myndigheter enligt förordning (EU) 2023/2854.

Utfärdad i Bryssel den 29 oktober 2026.

På kommissionens vägnar
Michael McGRATH
Ledamot av kommissionen

BILAGA I

ALLMÄN INLEDNING

1. **Bakgrund**

År 2022 inrättade kommissionen en expertgrupp bestående av experter som utsetts på personligt mandat för att stödja kommissionen i att tillhandahålla praktiska verktyg till marknadsaktörer som skulle utöva nya rättigheter och skyldigheter enligt förordning (EU) 2023/2854 (nedan kallad *dataförordningen*). Experterna utarbetade standardavtalsvillkor för åtkomst till och användning av data samt standardavtalsklausuler för databehandlingstjänster. Dessa standardavtalsvillkor och standardavtalsklausuler ingick i en rapport som offentliggjordes i april 2025 i gruppens register . Expertgruppen fick stöd av en undergrupp bestående av företag och europeiska samt nationella näringslivsorganisationer. Undergruppen gav experterna återkoppling under hela utarbetandet av utkastet.

För att ge experterna ytterligare underlag anordnade kommissionens avdelningar inte enbart riktade samråd, genom att testa utkastet till mallarna med företag som frivilligt ställde upp på detta, utan också två omgångar av offentliga samråd (en om den version av standardavtalsvillkor och standardavtalsklausuler som utarbetats av experterna och en om de slutliga versionerna som ingår i expertgruppens rapport).

På grundval av expertgruppens rapport och de synpunkter som inkom under de offentliga samråden och i enlighet med artikel 41 i dataförordningen utarbetade kommissionen de standardavtalsvillkor och standardavtalsklausuler som ingår som bilagor till denna rekommendation.

Standardavtalsvillkoren och standardavtalsklausulerna är inte bindande. De har utformats på ett sådant sätt att parterna kan anpassa dem efter sina avtalsmässiga behov. Parterna måste dock beakta att dessa standardavtalsvillkor och standardavtalsklausuler har utformats för att vara förenliga med de rättigheter och skyldigheter som föreskrivs i dataförordningen, och att de också har utformats för att vara förenliga med varandra. De innehåller information om deras frivilliga karaktär och råd till parterna om de rättsliga konsekvenserna av att göra ändringar. Dessutom bör tvistlösningsorgan som utsetts enligt artikel 10 i dataförordningen beakta standardavtalsvillkoren och standardavtalsklausulerna.

Standardavtalsvillkoren och standardavtalsklausulerna har utformats främst för avtalsförhållanden mellan företag. De kan emellertid också användas i förhållanden mellan företag och konsumenter. I så fall måste dock ytterligare bestämmelser läggas till för att avtalet ska överensstämma med obligatoriska konsumentskyddsregler (t.ex. konsumentens ångerrätt vid avtal som ingås online/på distans).

Användningen av dessa standardavtalsvillkor och standardavtalsklausuler befriar inte parterna från deras skyldighet att säkerställa efterlevnaden av tillämpliga tvingande bestämmelser i unionsrätten eller nationell rätt. Parterna har fullständig frihet att använda standardavtalsvillkoren och standardavtalsklausulerna. Kommissionen ansvarar inte för några konsekvenser som följer av användningen av klausulerna.

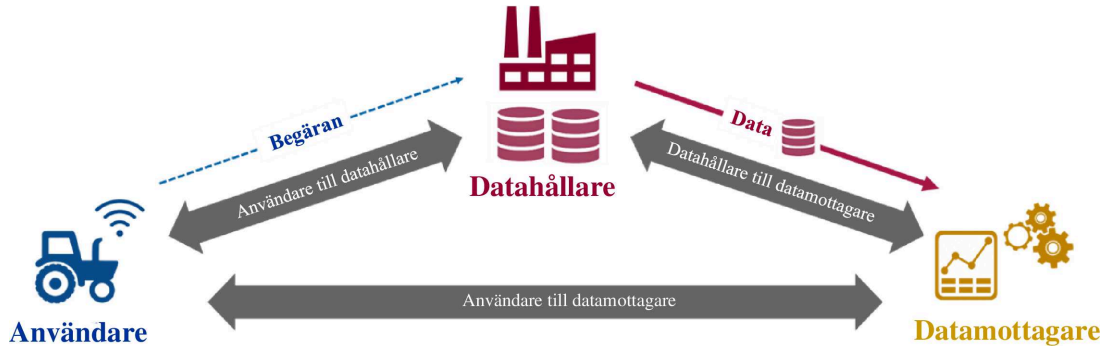
Kommissionen kan se över dessa standardavtalsvillkor och standardavtalsklausuler mot bakgrund av deras tillämpning och inverkan på företag och marknadspraxis.

2. **Standardavtalsvillkor**

De standardavtalsvillkor som anges i bilagorna II–V har utarbetats för att hjälpa parterna att utforma och förhandla fram avtal om åtkomst till och användning av data (personuppgifter och icke-personuppgifter). Syftet med dessa avtal är att säkerställa rättvisa, rimliga och icke-diskriminerande avtalsenliga rättigheter och skyldigheter, inbegripet rimlig ersättning och skydd av företagshemligheter.

De avtalsslutande parterna definieras i början av varje standardavtalsvillkor, i förekommande fall i enlighet med de termer som definieras i dataförordningen: data, datahållare, användare, datamottagare osv.

Vilka standardavtalsvillkor ska användas för vilken typ av datadelning?



Standardavtalsvillkoren i bilaga II har utformats för avtal mellan en datahållare och en användare av en uppkopplad produkt eller tillhörande tjänst, där datahållaren vill använda data som genereras med hjälp av produkten/tjänsten.

Standardavtalsvillkoren i bilaga III har utformats för avtal mellan en användare av en uppkopplad produkt eller tillhörande tjänst och en tredjepartsdatamottagare, där användaren begär att en datahållare ska göra data tillgängliga för en datamottagare enligt artikel 5 i dataförordningen.

Standardavtalsvillkoren i bilaga IV har utformats för avtal mellan en datahållare och en tredjepartsdatamottagare som är ett företag, där en datahållare är skyldig (enligt artikel 5 i dataförordningen) att göra data tillgängliga för en mottagare när en användare av produkten begär detta. Villkoren kan också användas med lämpliga ändringar när en datahållare är skyldig att göra data tillgängliga för en tredjepartsdatamottagare enligt annan unionsrätt eller nationell lagstiftning som antagits enligt unionsrätten.



Standardavtalsvillkoren i bilaga V har utformats för avtal mellan en datadelare och en datamottagare där datadelaren vill göra data tillgängliga för en datamottagare frivilligt och oberoende av någon begäran från en användare eller liknande part. Termen *datadelare* valdes för att ta hänsyn till de många scenarier som är möjliga här.

Parterna bör identifiera sin egen situation med hänvisning till de olika scenarier som förklaras ovan och sedan använda relevanta standardavtalsvillkor.

Standardavtalsvillkorens rättsliga värde i förhållande till dataförordningen och annan tillämplig lagstiftning

De avtalsslutande parternas användning av standardavtalsvillkoren påverkar inte deras rättigheter och skyldigheter enligt dataförordningen eller annan unionsrätt eller medlemsstaternas nationella lagstiftning som antagits i enlighet med unionsrätten, inbegripet den personuppgiftsansvariges skyldigheter och de registrerades rättigheter enligt förordning (EU) 2016/679, och enligt konkurrenslagstiftningen.

Parterna bör vara särskilt uppmärksamma när delningen av data avser personuppgifter eller blandade datamängder. I synnerhet måste datahållare göra personuppgifter tillgängliga för användare eller tredje parter, i enlighet med förordning (EU) 2023/2854, men endast så länge det finns en rättslig grund i enlighet med förordning (EU) 2016/679.

Liksom för alla avtal hindrar inte parternas användning av standardavtalsvillkoren en behörig domstol eller administrativ myndighet från att ogiltigförklara avtalet eller vissa villkor i detta på grund av bristande överensstämmelse med unionsrätten eller medlemsstaternas nationella lagstiftning.

3. **Standardavtalsklausuler**

Dessa standardavtalsklausuler är avsedda att hjälpa parterna med det avtalsmässiga genomförandet av de rättigheter och skyldigheter som följer av dataförordningen. Standardavtalsklausulerna är en uppsättning modulära klausuler som kompletterar varandra men som också kan användas separat. De är avsedda att införas i avtal om databehandlingstjänster.

Standardavtalsklausulerna syftar till att hjälpa kunder och leverantörer av alla databehandlingstjänster som omfattas av dataförordningen, oavsett om de är offentliga, privata eller andra, små, medelstora eller stora.

I enlighet med dataförordningens definition av en databehandlingstjänst är dessa standardavtalsklausuler tillämpliga på alla molntjänstmodeller, inklusive infrastruktur som en tjänst (IaaS), plattform som en tjänst (PaaS) och programvara som en tjänst (SaaS), där de uppvisar de egenskaper som fastställs i artikel 2.8 i dataförordningen.

De standardavtalsklausuler som omfattas av dataförordningen innehåller inte kraven i den allmänna dataskyddsförordningen ([1]). Avtalsbestämmelser för att säkerställa efterlevnaden av den allmänna dataskyddsförordningen bör inkluderas i avtalet. Kommissionen har antagit standardavtalsklausuler för förhållandet mellan den personuppgiftsansvarige och personuppgiftsbiträdet för att underlätta både för efterlevnaden av den allmänna dataskyddsförordningen och för överföring av personuppgifter till länder utanför EES ([2]).

De standardavtalsklausuler som ingår i dataskyddsförordningen gör det möjligt för de enheter som använder dem att säkerställa och visa att de uppfyller vissa krav i dataskyddsförordningen. Dessa standardavtalsklausuler kan inte ändras av parterna, men de kan inkluderas i ett bredare avtal eller användas som ett fristående avtal.

Hur använder man standardavtalsklausulerna?

Även om det rekommenderas att använda hela uppsättningen standardavtalsklausuler är det viktigt att notera att dessa standardavtalsklausuler inte utgör hela avtalet om databehandlingstjänster som skulle gälla mellan en kund och en leverantör. Övriga frågor som inte behandlas i dataförordningen och standardavtalsklausulerna måste ingå i ett sådant avtal.

Ett antal definitioner som används i de olika standardavtalsklausulerna och som är anpassade till dataförordningen finns i bilaga XII. Om andra definitioner än de som föreslås i standardavtalsklausulerna används, måste standardavtalsklausulerna anpassas i enlighet med dessa. Detta är bara ett exempel på anpassningar som är möjliga samtidigt som man fortfarande använder hela uppsättningen eller en del av standardavtalsklausulerna.

För att underlätta läsningen innehåller standardavtalsklausulerna korshänvisningar som kopplar vissa bestämmelser i standardavtalsklausulerna till relevanta bestämmelser i dataförordningen eller till andra standardavtalsklausuler.

Det kan finnas ytterligare regler och krav som är tillämpliga på databehandlingstjänster i specifika sektorer som också bör beaktas (till exempel inom finanstjänster, hälso- och sjukvård, telekommunikation, industri, energi eller den offentliga sektorn). Dataförordningen innehåller undantag från vissa skyldigheter som rör standardavtalsklausulerna om byte och utträde. Ytterligare förklaringar finns i standardavtalsklausulerna om byte och utträde.

Dataförordningen innehåller följande specifika möjligheter att hantera tvister:

Kunder och leverantörer har tillgång till ett tvistlösningsorgan som utsetts av medlemsstaterna i enlighet med artikel 10.4 i dataförordningen.

Var och en av parterna kan lämna in ett klagomål till den behöriga myndigheten i sin medlemsstat i enlighet med artikel 37.5 b i dataförordningen.

([1]) Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), (EUT L 119, 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([2]) Publikationer om standardavtalsklausuler – Europeiska kommissionen.

Vid utseendet fastställer medlemsstaterna dock den berörda behöriga myndighetens arbetsuppgifter och befogenheter som kan variera i viss utsträckning mellan olika medlemsstater. Det är möjligt att en sådan myndighet inte är behörig att lösa alla tvister mellan kunden och leverantören. Parterna måste bedöma det lämpligaste sättet att ålägga den andra parten att fullgöra sina rättsliga och avtalsenliga skyldigheter och hur tvister ska lösas.

Parterna kan komma överens om att täcka flera tjänster i ett enda avtal, som kan kallas *ramavtal om tjänster* eller ges en annan titel (*avtalet*). Detta är ytterligare ett skäl till varför det rekommenderas att lägga till standardavtalsklausuler i avtalet. Om det täcker alla tjänster och kunden beslutar att byta en eller ett visst antal tjänster, kommer avtalet att fortsätta att gälla för de andra tjänsterna.

Om parterna avser att använda dessa standardavtalsklausuler endast delvis eller att göra ändringar i dem, bör de noga överväga hur detta kan påverka de avtalsenliga rättigheterna och skyldigheterna. Juridisk och annan professionell rådgivning rekommenderas alltid i sådana situationer.

BILAGA II

STANDARDAVTALSVILLKOR

för avtal om åtkomst till och användning av data mellan datahållare och användare av uppkopplade produkter och tillhörande tjänster

Dessa standardavtalsvillkor är avsedda att reglera åtkomst till och användning av data samt därmed sammanhängande avtalsfrågor som kan uppstå mellan en datahållare och användare (enligt definitionen i förordning (EU) 2023/2854, nedan kallad *dataförordningen*).

Det viktigaste i dataförordningen i detta avseende är att

— användare ges rätt att få åtkomst till data som genereras av deras uppkopplade produkter och/eller tillhörande tjänster (med skyddsåtgärder för data som skyddas som företagshemligheter),

— användare också kan dela dessa uppgifter med tredje part, t.ex. för att dra nytta av eftermarknadstjänster,

— datahållaren måste ingå ett avtal med användaren för att använda och dela icke-personuppgifter, och

— oskäliga avtalsvillkor om åtkomst till och användning av data, eller ansvar och rättsmedel vid överträdelse eller uppsägning av datarelaterade skyldigheter, inte är bindande om de har påtvingats ett företag ensidigt av ett annat företag.

Detta avtal har en modulär struktur och kan användas som ett fullständigt avtal, men parterna kan också välja vissa klausuler som passar deras specifika situation. Vissa villkor är kanske inte relevanta för alla produkter och alla avtal, t.ex. de som rör skydd av företagshemligheter eller tillämpning av tekniska skyddsåtgärder. Dessa bör endast inkluderas i avtalet av parterna när det är relevant. På samma sätt bör begränsningar av åtkomst till, användning av eller delning av data endast inkluderas i avtalen när det är relevant, dvs. om produktens säkerhetskrav annars skulle undergrävas, vilket skulle få allvarliga negativa konsekvenser för fysiska personers hälsa, säkerhet eller trygghet.

Flera klausuler innehåller alternativ, och här bör parterna överväga sina specifika behov, affärsförbindelser och intressen för att identifiera det alternativ som bäst passar deras avtal.

Vissa klausuler är också markerade *(om tillämpligt)* och bör inkluderas om vissa villkor är uppfyllda.

Även om kommissionen rekommenderar standardavtalsvillkoren är de inte bindande och parterna kan alltid göra undantag från dem.

1. Parter och produkt/tillhörande tjänst(er)

1.1. Avtalsparter

Detta avtal om åtkomst till och användning av data ingås

mellan

(ange namn, kontaktuppgifter och ytterligare referenser) (*datahållaren*)

Enligt dataförordningen avses med *datahållare* ”en fysisk eller juridisk person som har en rätt eller skyldighet, i enlighet med [dataförordningen], tillämplig unionsrätt eller nationell lagstiftning som antagits i enlighet med unionsrätten, att använda och tillgängliggöra data, inbegripet produktdata eller data från tillhörande tjänster som denne har hämtat eller genererat under tillhandahållandet av en tillhörande tjänst, om detta avtalats”.

I de flesta fall kan datahållaren vara tillverkaren av produkten eller leverantören av den relevanta tillhörande tjänsten, eller en annan part som samarbetar med tillverkaren eller leverantören och som kan hämta data från produkten eller den tillhörande tjänsten.

Om fler än en part kan vara datahållare kan detta hanteras på olika sätt, till exempel genom att

(a) var och en av parterna ingår ett eget avtal med användaren som oberoende datahållare, eller
(b) en av parterna ingår ett avtal med användaren och därmed agerar som datahållare. I avsaknad av ett avtal med användaren anses de andra parterna vara tredje parter i den mening som avses i klausul 3.2. Baserat på avtalet med användaren och på avtal med dessa tredje parter kan datahållaren samordna åtkomst till och användning av data.

Vilken av de två möjligheterna som är att föredra i ett givet fall beror på många faktorer. Parterna kan till exempel överväga om användarna föredrar att ha endast en avtalsslutande part och ett avtal. Parterna bör vara medvetna om att det finns ett nära samband mellan valet mellan de två alternativen och hur parterna formulerar klausul 3.2.1.

och

[ALTERNATIV 1] [(*ange namn, kontaktuppgifter och ytterligare referenser*) (*användaren*)]

[ALTERNATIV 2] [varje part som identifierar sig som användare i den mening som avses i dataförordningen och som samtycker till villkoren i detta avtal genom att vidta följande åtgärder: [*ange tekniska åtgärder som ska vidtas av varje part som uppfyller kraven för att betraktas som användare, t.ex. information som ska lämnas och bekräftelser som ska göras via ett användargränssnitt*) (*användaren*)]

i detta avtal gemensamt benämnda *parterna* och var för sig *parten*.

Enligt dataförordningen avses med *användare* ”en fysisk eller juridisk person som äger en uppkopplad produkt eller till vilken tillfälliga rättigheter att använda den uppkopplade produkten har överlåtits genom avtal eller som erhåller tillhörande tjänster”. Detta avtal kan bli relevant i ett stort antal olika sammanhang. Å ena sidan finns det fall där användaren är känd för datahållaren och där advokater på båda sidor förhandlar fram ett skräddarsytt avtal om åtkomst till och användning av data (t.ex. ett flygbolag som köper flygplan av en flygplanstillverkare). Å andra sidan finns det fall där massprodukter och tjänster lanseras till miljontals konsumenter vars identitet inte är känd (och vars identitet vi kanske inte ens vill lämna ut av dataskyddsskäl) och där individuella förhandlingar helt enkelt är omöjliga (t.ex. uppkopplade kaffemaskiner).

För den senare typ av fall, och många andra fall mellan dessa ytterligheter, kan det vara till hjälp att identifiera användaren inte genom namn utan genom vidtagna åtgärder (t.ex. att skapa ett användarkonto eller helt enkelt ansluta en uppkopplad kaffemaskin och godkänna villkoren genom att klicka på ”OK” på en skärm). Parterna bör vara medvetna om att domstolar, särskilt i fall där konsumenter är inblandade, kommer att bedöma om förfarandet är utformat på ett sätt som överensstämmer med reglerna i tillämplig allmän avtalsrätt och konsumenträtt, enligt vilka villkor kan behöva inkluderas i avtalet.

1.2. **Produkt/tillhörande tjänst(er)**

Detta avtal ingås med avseende på

(a) följande uppkopplade produkt(er) (*produkten*): (ange namn och ytterligare uppgifter om den specifika uppkopplade produkt eller typ av produkter som omfattas av detta avtal),

(b) följande tillhörande tjänst(er) (*tillhörande tjänst(er)*): (ange namn och ytterligare uppgifter om de specifika tillhörande tjänster eller typ av tillhörande tjänster som omfattas av detta avtal, om tillämpligt).

1.2.1. Användaren försäkrar att han/hon antingen är ägare till produkten eller har avtalsenlig rätt att använda produkten enligt ett hyresavtal, leasingavtal eller liknande avtal och/eller att erhålla den/de relaterade tjänsten/tjänsterna enligt ett serviceavtal.

[ALTERNATIV 1] [Användaren förbinder sig att på vederbörligen motiverad begäran tillhandahålla datahållaren all relevant dokumentation som styrker dessa förklaringar, där så är nödvändigt.]

[ALTERNATIV 2] [Dokumentation som styrker dessa förklaringar samt uppgifter om vem som ska betraktas som användare enligt detta avtal finns i **tillägg 9**.]

Enligt dataförordningen får datahållaren inte kräva att en fysisk eller juridisk person lämnar någon information utöver vad som är nödvändigt för att kontrollera om en person kan anses vara användare i dataförordningens mening. I många situationer, särskilt när det gäller masskonsumtionsvaror eller företagsutrustning med relativt låg känslighet för de data som genereras (t.ex. uppkopplade kaffemaskiner, se ovan), är det normalt oproportionerligt att göra ytterligare begäranden.

2. **Data som omfattas av avtalet**

De data som omfattas av detta avtal består av alla lätt åtkomliga produktdata eller data från tillhörande tjänster i den mening som avses i dataförordningen, och inkluderar både icke-personuppgifter och personuppgifter (*data*).

Datahållaren listar data i **tillägg 1**, med en beskrivning av typ eller karaktär, uppskattad volym, insamlingsfrekvens, lagringsplats och lagringstid för data.

Om andra data än de som anges i tillägg 1 måste göras tillgängliga för användaren under avtalets giltighetstid, kommer **tillägg 1** att ändras i enlighet därmed.

Enligt dataförordningen avses med ***produktdata*** ”data som genereras genom användning av en uppkopplad produkt och som tillverkaren har utformat för att kunna hämtas via en elektronisk kommunikationstjänst, via fysisk åtkomst eller åtkomst i enheten av en användare, datahållare eller en tredje part, inbegripet tillverkaren i tillämpliga fall”.

Med ***data från en tillhörande tjänst*** avses ”data som representerar digitaliseringen av användaråtgärder eller användarhändelser som kan härledas från den uppkopplade produkten och som registreras avsiktligt av användaren eller genereras som en biprodukt av användarens åtgärder under leverantörens tillhandahållande av en tillhörande tjänst”.

Produktdata och data från en tillhörande tjänst kan vara både personuppgifter och icke-personuppgifter. De omfattar ”data i obearbetad form” samt ”data som har förbehandlats i syfte att göra dem begripliga och användbara för senare behandling”. De omfattar dock inte ”[i]nformation som avleds eller härleds från sådana data, som är resultatet av ytterligare investeringar i tilldelning av värden eller insikter från dessa data” (skäl 15).

Lätt åtkomliga data omfattar ”produktdata och data från en tillhörande tjänst som en datahållare lagligen erhåller eller lagligen kan erhålla från den uppkopplade produkten eller tillhörande tjänsten, utan oproportionella ansträngningar som går utöver en enkel åtgärd”.

Som förklaras i skälen omfattar denna definition inte ”data som genereras genom användning av en uppkopplad produkt om den uppkopplade produkten inte har utformats för att lagra eller överföra sådana data utanför den komponent i vilken de genereras eller den uppkopplade produkten som helhet” (skäl 20). ”Tillverkarnas val av utformning och, i förekommande fall, unionsrätt eller nationell rätt som tillgodoser sektorsspecifika behov samt mål eller relevanta beslut från behöriga myndigheter bör avgöra vilka data en uppkopplad produkt kan göra tillgängliga.” (skäl 14).

3. **Datahållarens användning och delning av data**

3.1. **Datahållarens överenskomna användning av icke-personuppgifter**

3.1.1. Utan att det påverkar någon laglig rätt att använda data, förbinder sig datahållaren att använda data som inte är personuppgifter endast för de ändamål som överenskommits med användaren enligt följande:

(a) Fullgöra ett avtal med användaren eller verksamhet som är relaterad till sådant avtal (t.ex. utfärda fakturor, skapa och tillhandahålla rapporter eller analyser, finansiella prognoser, konsekvensbedömningar, beräkna personalförmåner).

(b) Tillhandahålla support, garanti, säkerhet eller liknande verksamhet eller bedöma användares, datahållares eller tredje parts anspråk (t.ex. avseende produktens funktionsfel) som rör produkten eller tillhörande tjänst.

(c) Övervaka och upprätthålla produktens eller tillhörande tjänstens funktion, säkerhet och skydd samt säkerställa kvalitetskontroll.

(d) Förbättra funktionen hos alla produkter eller tillhörande tjänster som erbjuds av datahållaren.

(e) Utveckla nya produkter eller tjänster av datahållaren, av tredje parter som agerar på datahållarens vägnar (dvs. där datahållaren beslutar vilka arbetsuppgifter som ska anförtros sådana parter och vilka fördelar som ska dras av detta), i samarbete med andra parter eller genom företag med särskilt syfte (t.ex. gemensamma företag).

(f) Aggregera dessa data med andra data eller skapa härledda data, för alla lagliga ändamål, även i syfte att sälja eller på annat sätt göra sådana aggregerade eller härledda data tillgängliga för tredje part, förutsatt att sådana data inte gör det möjligt att identifiera specifika data som överförs till datahållaren från den uppkopplade produkten eller gör det möjligt för en tredje part att härleda dessa data från datamängden.

Parterna bör ange syftena för vilka och samtliga detaljer om hur datahållaren får använda icke-personuppgifter. Förteckningen omfattar de vanligaste användningsområdena, men parterna kan fritt välja bland de som anges i denna klausul eller lägga till ytterligare användningsområden.

När parterna kommer överens om användningen av data kan de gruppera dessa data i kategorier, om så är lämpligt. Bredare kategorier kan exempelvis omfatta

— produkt- eller tjänstestatusdata (t.ex. konfiguration, version, diagnostiska meddelanden, förbrukningsdata, underhållsdata),

— kundens användningsdata (t.ex. aktivitetstider, aktivitetstyper, produktens geografiska position) – observera att dessa data i vissa fall kan utgöra personuppgifter och inte omfattas av denna klausul utan av klausul 3.3 och andra bestämmelser i avtalet,

— data om användarmiljö (t.ex. markförhållanden, arealstorlek),

— allmänna miljödata (t.ex. väderdata).

Parterna bör vara medvetna om att standardformuleringen ovan i denna uppsättning villkor förutsätter att de syften som anges där är de syften som eftersträvas av den datahållare som är part i detta avtal. När det gäller utveckling av nya produkter eller tjänster antas till exempel att utvecklingsverksamheten bedrivs av datahållaren, om än eventuellt tillsammans med andra parter, såsom en komponenttillverkare. Delning av data med sådana parter bör därför vara tillåten som standard, i enlighet med vad som anges i klausul 3.2.1 a i och ii.

Användning av data för oberoende ändamål av tredje part skulle kräva att dessa tredje parter ingår ett separat avtal med användaren eller att den valfria klausulen 3.2.1 a iii, som tillåter datahållaren att sälja eller donera data till sådana tredje parter för deras egna ändamål, tillämpas.

Användaren bör bedöma konsekvenserna av sådan användning av datahållaren eller tredje part för sin verksamhet och sina intressen, särskilt om de bör ersättas av datahållaren, till exempel när datahållaren kan sälja de data som genererats av användaren till tredje part.

3.1.2. Datahållaren förbinder sig att inte använda dessa data

(a) för att få insikter om användarens ekonomiska situation, tillgångar och produktionsmetoder, eller om användarens användning av produkten eller den tillhörande tjänsten på något annat sätt som kan undergräva användarens kommersiella ställning på de marknader där användaren är verksam,

(b) [ALTERNATIV] (*ange användningar av data som till exempel avsevärt skadar användarens berättigade intressen*)].

Parterna kanske vill ange mer detaljerat vilken typ av dataanvändning de anser vara så skadlig att den måste uteslutas. Detta beror på den relevanta sektorn och andra omständigheter. Användaren kanske särskilt vill utesluta

— användning av särskilda kategorier av mycket känsliga data, och/eller

— användning av data för särskilda ändamål.

Ingen av de användningar av data som överenskommits enligt klausul 3.1.1 får strida mot denna klausul, och datahållaren åtar sig att genom lämpliga avtalsmässiga, organisatoriska och tekniska åtgärder säkerställa att ingen tredje part inom datahållarens organisation använder data på detta sätt.

3.2. **Delning av icke-personuppgifter med tredje part och användning av behandlingstjänster**

3.2.1. Utan att det påverkar de rättsliga kraven enligt unionsrätten eller nationell rätt för en datahållare att göra data tillgängliga, får datahållaren dela icke-personuppgifter med tredje part om

(a) dessa används av tredje part uteslutande för att

i) hjälpa datahållaren att uppnå de syften som är tillåtna enligt klausul 3.1.1,

ii) i samarbete med datahållaren eller genom företag med särskilt syfte uppnå de syften som är tillåtna enligt klausul 3.1.1,

iii) [ALTERNATIV] [(ange de syften som tredje part kan eftersträva för sina egna behov, oberoende av datahållaren, och om data delas för dessa syften mot ersättning eller gratis),] och

(b) datahållaren förbinder tredje part genom avtal

i) att inte använda dessa data för några ändamål eller på något sätt som går utöver den användning som är tillåten enligt föregående klausul 3.2.1 a,

ii) att följa innehållet i klausul 3.1.2,

iii) att tillämpa de skyddsåtgärder som krävs enligt klausul 3.4.1, och

iv) [ALTERNATIV 1] [att inte dela dessa data med någon annan om inte användaren ger sitt generella eller specifika samtycke till sådan vidare överföring. Datahållaren måste ålägga den tredje part som man delar data med att inkludera klausulerna motsvarande punkterna i–iv i sina avtal med mottagarna.] [ALTERNATIV 2] [att inte dela dessa data med någon annan utom i de fall som anges i tillägg 5.]

[ALTERNATIV] [Ytterligare detaljer, inklusive identitet eller kategorier av tredje parter med vilka data kan delas, begränsningar av tredje parters användning av data, samt ytterligare villkor och skyddsåtgärder, anges i detalj i **tillägg 5**.]

3.2.2. Utan hinder av klausul 3.2.1 får datahållaren använda behandlingstjänster, t.ex. molntjänster (inklusive infrastruktur som en tjänst, plattform som en tjänst och programvara som en tjänst), värdtjänster eller liknande tjänster för att för egen räkning och på eget ansvar uppnå de överenskomna syftena enligt klausul 3.1.1. Tredje parter får också använda sådana tjänster för att för egen räkning och på eget ansvar uppnå de överenskomna syftena enligt klausul 3.2.1 a.

3.3. **Datahållarens användning och delning av personuppgifter**

3.3.1. Datahållaren får använda, dela med tredje part eller på annat sätt behandla personuppgifter endast om det finns en rättslig grund och på de villkor som tillåts enligt Europaparlamentets och rådets förordning (EU) 2016/679 ([1]) (allmänna dataskyddsförordningen) och, i förekommande fall, direktiv 2002/58/EG (direktivet om integritet och elektronisk kommunikation).

([1]) Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter, om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

3.4. **Skyddsåtgärder som vidtas av datahållaren**

3.4.1. Datahållaren åtar sig att tillämpa skyddsåtgärder för att förhindra förlust av data och obehörig åtkomst till data [ALTERNATIV 1] [som är rimliga och lämpliga under omständigheterna, med hänsyn till den vetenskapliga och tekniska utvecklingen, den potentiella skada som användaren kan drabbas av och kostnaderna för skyddsåtgärderna]. [ALTERNATIV 2] [som beskrivs i detalj i tillägg 6.]

Parterna bör överväga om de vill inkludera, vid behov i ett separat tillägg, alla detaljer om hur användarens viktiga intressen kan skyddas på ett effektivt sätt. Åtgärderna kan vara både tekniska (t.ex. kryptering, brandväggar, delad lagring) och organisatoriska (t.ex. involvering av en betrodd tredje part). Eftersom åtgärderna måste vara proportionerliga kommer deras innehåll att variera kraftigt beroende på vilken typ av data det rör sig om och vilka intressen som står på spel.

4. ***(om tillämpligt)* Användarens åtkomst till data på begäran**

Dessa klausuler i avsnitt 4 gäller om användaren inte kan få direkt åtkomst till data från produkten eller den tillhörande tjänsten i enlighet med artikel 3 i dataförordningen. I så fall har användaren rätt att på begäran få åtkomst till data från datahållaren, i enlighet med artikel 4 i dataförordningen. Om användaren vill ge åtkomst till data till en datamottagare gäller klausulerna i avsnitt 7 nedan.

4.1. **Skyldighet att göra data tillgängliga**

4.1.1. Data, tillsammans med relevanta metadata som är nödvändiga för att tolka och använda dessa data, måste göras tillgängliga för användaren av datahållaren, på begäran av användaren eller en part som agerar på dennes vägnar. Begäran kan meddelas genom (*beskriv förfarandet för en enkel begäran via elektroniska medel där detta är tekniskt genomförbart*). För att kontrollera att begäran görs av användaren får datahållaren inte kräva mer information än vad som är nödvändigt. *(om tillämpligt)* [Om begäran görs av en part som agerar på användarens vägnar ska en fullmakt bifogas begäran.]

Tillägg 2 visar vilka uppgifter en begäran kan innehålla.

4.1.2. När användaren inte är den registrerade ska datahållaren endast göra personuppgifter tillgängliga för användaren när det finns en giltig rättslig grund för att göra personuppgifter tillgängliga enligt artikel 6 i förordning (EU) 2016/679 och endast när, i förekommande fall, de villkor som anges i artikel 9 i den förordningen och artikel 5.3 i direktiv 2002/58/EG (direktivet om integritet och elektronisk kommunikation) är uppfyllda.

I detta avseende måste användaren, när denne inte är den registrerade, i varje begäran som framställs enligt föregående klausul ange den rättsliga grunden för behandlingen enligt artikel 6 i förordning (EU) 2016/679 (och, i förekommande fall, det tillämpliga undantaget enligt artikel 9 i den förordningen och artikel 5.3 i direktiv 2002/58/EG) som ligger till grund för begäran om att personuppgifter ska göras tillgängliga.

4.2. **Dataegenskaper och villkor för åtkomst**

4.2.1. Datahållaren måste göra data tillgängliga för användaren utan kostnad för användaren, med data av minst samma kvalitet som när de blir tillgängliga för datahållaren, och i alla händelser i ett heltäckande, strukturerat, allmänt använt och maskinläsbart format.

Med *metadata* avses en strukturerad beskrivning av innehållet i eller användningen av data som underlättar sökandet efter eller användningen av dessa data. Enligt artikel 4.1 i dataförordningen måste metadata göras tillgängliga tillsammans med data, i den mån metadata är ”nödvändiga för att tolka och använda” data.

Även om de relevanta metadata som behövs för att tolka och använda dessa data inte fastställs och därför måste identifieras från fall till fall, anges i dataförordningen att ”d[e] data som ska göras tillgängliga bör innefatta relevanta metadata, bland annat grundläggande information om sammanhang och tidsstämpel, för att göra datan användbar när den kombineras med andra data, såsom data sorterade och klassificerade med andra relaterade datapunkter, eller omformateras till ett allmänt använt format” (skäl 15).

Datahållaren och användaren får använda sig av tjänster från en tredje part (inklusive en tredje part som tillhandahåller dataförmedlingstjänster enligt definitionen i artikel 2 i Europaparlamentets och rådets förordning (EU) 2022/868 ([2])) för att möjliggöra utövandet av användarens rättigheter enligt klausul 4.1 i detta avtal. En sådan tredje part ska inte betraktas som en datamottagare enligt dataförordningen, och sådana tjänster kan erbjudas av en leverantör som betraktas som en grindvakt enligt artikel 3 i förordning (EU) 2022/1925, såvida leverantören inte behandlar data för egna affärsändamål.

En tredje part som tillhandahåller en tjänst på datahållarens eller användarens vägnar kommer inte att betraktas som en datamottagare enligt dataförordningen, och dessa tjänster kan erbjudas av en leverantör som betraktas som en grindvakt enligt artikel 3 i Europaparlamentets och rådets förordning (EU) 2022/1925 ([3]), såvida leverantören inte behandlar data för egna affärsändamål.

4.2.2. Användaren måste få åtkomst till begärda data

a) enkelt och säkert,

b) utan oskäligt dröjsmål,

(om tillämpligt) [c) kontinuerligt och i realtid].

4.2.3. För att uppfylla kraven i klausulerna 4.2.1 och 4.2.2 specificerar datahållaren dessa villkor för åtkomst i tillägg 1.

Enligt artikel 4.1 i dataförordningen ska data göras tillgängliga utan oskäligt dröjsmål samt, i tillämpliga fall och där så är tekniskt genomförbart, kontinuerligt och i realtid.

Eftersom det finns olika sätt att genomföra dessa rättsliga krav, bör datahållaren specificera alla detaljer om hur åtkomst ska tillhandahållas i tillägg 1. Villkoren för åtkomst får inte undergräva någon av de rättigheter som användaren har enligt dataförordningen eller annan tillämplig lagstiftning.

Med hänsyn till denna begränsning bör datahållaren som ett första steg besluta om man vill tillhandahålla

— fullständig överföring av data, dvs. en kopia av data överförs till ett medium som kontrolleras av användaren

— genom överföring som initieras av datahållaren (push), t.ex. onlineöverföring, uppladdning till användarens molnutrymme eller leverans av ett fysiskt medium på vilket data lagras, eller

— genom hämtning som initieras av användaren (pull), t.ex. genom tillhandahållande av ett API, åtkomst till datahållarens molnutrymme eller liknande verktyg som gör det möjligt för användaren att få åtkomst till och extrahera data, eller

— åtkomst till data där de lagras, dvs. data nås och behandlas på ett medium som kontrolleras av datahållaren eller en betrodd tredje part, t.ex. genom att användaren loggar in på ett särskilt utrymme på datahållarens eller den betrodda tredje partens servrar, men data överförs inte till ett medium som kontrolleras av användaren, såvida inte särskilda arrangemang har gjorts.

Fullständig överföring ger användaren maximal frihet, medan åtkomst till den plats där data lagras ökar risken för användarna att deras affärsidéer blir kända. Enligt artikel 13.5 e i dataförordningen ska dessutom ”ett avtalsvillkor […] antas vara oskäligt […] om det har till syfte eller verkan att […] hindra den part som ensidigt har ålagts villkoret att erhålla en kopia av de data som den parten har tillhandahållit eller genererat under avtalets löptid eller inom en rimlig tidsperiod efter det att avtalet sagts upp”. Fullständig överföring bör därför vara standardregeln.

([2]) Europaparlamentets och rådets förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten) (EUT L 152, 3.6.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/868/oj).

([3]) Europaparlamentets och rådets förordning (EU) 2022/1925 av den 14 september 2022 om öppna och rättvisa marknader inom den digitala sektorn och om ändring av direktiv (EU) 2019/1937 och (EU) 2020/1828 (förordningen om digitala marknader) (EUT L 265, 12.10.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/1925/oj).

Fullständig överföring minskar dock avsevärt datahållarens möjlighet att förhindra missbruk och skydda sina intressen, t.ex. företagshemligheter. Därför bör det också vara möjligt att få åtkomst till och behandla de data som lagras. För att förena sådan åtkomst med användarens intressen är det ofta att föredra att få åtkomst till de data som lagras på ett medium som kontrolleras av en betrodd tredje part framför åtkomst till ett medium som kontrolleras av datahållaren. Åtkomst till den plats där data lagras bör normalt fortfarande innebära fjärråtkomst, och åtkomst på plats bör begränsas till extrema situationer med högsta grad av känslighet.

Om åtkomst ges till den plats där data lagras finns det ett antal frågor att lösa, bland annat hur man kan säkerställa att användarens affärsidéer inte röjs och vilka data användaren får extrahera och överföra till ett medium som denne själv kontrollerar (t.ex. härledda eller avledda data som är resultatet av användarens behandling).

Enligt artikel 4.1 i dataförordningen ska data göras tillgängliga utan oskäligt dröjsmål och, i tillämpliga fall och där så är tekniskt genomförbart, kontinuerligt och i realtid. Därför bör datahållaren i tillägget ange om åtkomst kan ges kontinuerligt och i realtid, och om så inte är fallet, med vilken frekvens.

Datahållaren bör också överväga en rad ytterligare frågor, såsom vilka behörigheter som krävs för åtkomst och vilka och hur många av användarens anställda som får åtkomst till data.

4.2.4. Datahållaren måste utan extra kostnad tillhandahålla användaren den information som är nödvändig för åtkomst till data i enlighet med artikel 4 i dataförordningen.

Detta omfattar särskilt tillhandahållande av information som är lätt åtkomlig för datahållaren om eventuella rättigheter som tredje part kan ha avseende dessa data, såsom rättigheter för registrerade som följer av förordning (EU) 2016/679, eller omständigheter som kan ge upphov till sådana rättigheter.

Datahållaren specificerar denna information i **tillägg 1**.

Parterna är fria att komma överens om ytterligare stöd, utöver kraven i dataförordningen, utan kostnad eller mot en avgift.

4.2.5. Datahållaren förbinder sig att inte lagra någon information om användarens åtkomst till begärda data utöver vad som är nödvändigt för

(a) ett korrekt genomförande av i) användarens begäran om åtkomst och ii) detta avtal,

(b) säkerheten och underhållet av datainfrastrukturen,

(c) fullgörandet av datahållarens lagliga skyldigheter att lagra sådan information.

4.3. **Återkoppling**

Om användaren identifierar en incident som rör klausul 2 om de data som omfattas av avtalet, kraven i klausulerna 4.2.1 eller 4.2.2 eller i **tillägg 1** om dataegenskaper och villkor för åtkomst, och om användaren förser datahållaren med en detaljerad beskrivning av incidenten, måste datahållaren och användaren samarbeta i god tro för att identifiera orsaken till incidenten.

Om incidenten orsakades av att datahållaren inte fullgjort sina skyldigheter måste denne åtgärda överträdelsen utan oskäligt dröjsmål. Om datahållaren inte gör detta anses det vara en grundläggande underlåtenhet att fullgöra sina skyldigheter, och användaren kan åberopa klausul 12 i detta avtal. Om användaren anser att hans eller hennes åtkomsträttighet enligt artikel 4.1 i dataförordningen har kränkts, har användaren också rätt att lämna in ett klagomål till den behöriga myndigheten som utsetts i enlighet med artikel 37.5 b i dataförordningen.

Denna klausul ger datahållaren möjlighet att rätta till eventuella överträdelser av sina lagliga eller avtalsenliga skyldigheter. Om datahållaren inte gör detta utan oskäligt dröjsmål, kan användaren utnyttja de avtalsenliga rättsmedel som anges i avtalet i händelse av grundläggande underlåtenhet att fullgöra sina skyldigheter.

Om användaren anser att hans eller hennes åtkomsträttighet enligt artikel 4.1 i dataförordningen har kränkts, har användaren också rätt att lämna in ett klagomål till den behöriga myndigheten, som utsetts i enlighet med artikel 37.5 b i dataförordningen. Användaren bör dock vara medveten om att de exakta arbetsuppgifterna och befogenheterna för de behöriga myndigheter som utsetts i enlighet med artikel 37 kan variera mellan medlemsstaterna.

Användaren har alltid rätt att söka ett effektivt rättsmedel inför behörig domstol eller att hänskjuta tvisten till ett alternativt tvistlösningsorgan.
Användaren måste därför noga överväga vilket som är det lämpligaste sättet att ålägga datahållaren att fullgöra sina rättsliga och avtalsenliga skyldigheter.

4.4. **Ensidiga ändringar av datahållaren**

4.4.1. Datahållaren får ensidigt ändra specifikationerna för dataegenskaperna eller villkoren för åtkomst som anges i **tillägg 1**, om detta är objektivt motiverat av datahållarens normala affärsverksamhet, till exempel genom en teknisk modifiering på grund av en omedelbar säkerhetsrisk i produktlinjen eller tillhörande tjänster eller en förändring i datahållarens infrastruktur. Alla ändringar måste uppfylla kraven i klausulerna 4.2.1 och 4.2.2.

Datahållaren måste meddela användaren om ändringen minst (*ange en rimlig tidsperiod*) innan ändringen träder i kraft.

En kortare tidsfrist kan vara tillräcklig

(a) om ändringen inte påverkar användarens åtkomst till och användning av data negativt, eller

(b) om ett sådant meddelande skulle vara omöjligt eller orimligt under omständigheterna, till exempel om omedelbara ändringar krävs på grund av en säkerhetsbrist som just har upptäckts.

5. **(om de data som datahållaren tillhandahåller på begäran av användaren måste skyddas som företagshemligheter) Skydd av företagshemligheter**

1. **Delning av företagshemligheter** – Datahållare kan i princip inte avslå en begäran om åtkomst till data enligt dataförordningen enbart på grundval av att vissa data anses vara skyddade som företagshemligheter, eftersom detta skulle undergräva dataförordningens avsedda verkningar.

Se klausul 5.1.

Företagshemligheter – Om datahållaren dock fastställer att vissa data som omfattas av detta avtal är skyddade som företagshemligheter enligt definitionen i direktiv (EU) 2016/943 ([4]) (nedan kallat *direktivet om företagshemligheter*) har datahållaren vissa rättigheter, främst rätten att fortsätta att bevara konfidentialiteten för de aktuella hemligheterna.

Enligt artikel 2.1 i direktivet om företagshemligheter avses med *företagshemlighet* information som uppfyller tre krav: a) Den är hemlig i den meningen att den inte, som helhet eller i den form dess beståndsdelar ordnats och satts samman, är allmänt känd hos eller lättillgänglig för personer i de kretsar som normalt sett handskas med typen av information i fråga. b) Den har kommersiellt värde på grund av att den är hemlig. c) Den person som lagligen kontrollerar den har med hänsyn till omständigheterna vidtagit rimliga åtgärder för att hålla den hemlig.

Med *innehavare av en företagshemlighet* avses en fysisk eller juridisk person som lagligen kontrollerar en företagshemlighet.

([4]) Europaparlamentets och rådets direktiv (EU) 2016/943 av den 8 juni 2016 om skydd mot att icke röjd know-how och företagsinformation (företagshemligheter) olagligen anskaffas, utnyttjas och röjs (EUT L 157, 15.6.2016, s. 1, ELI: http://data.europa.eu/eli/dir/2016/943/oj).

Data kan endast identifieras som företagshemligheter om de skyddas som sådana av datahållaren eller innehavaren av företagshemligheten när en begäran om åtkomst till data görs i enlighet med artikel 4 i dataförordningen.

Se klausul 5.1.1.

2. **Initial identifiering av företagshemligheter** – Datahållarnas rättigheter avseende företagshemligheter är – initialt – endast tillämpliga om och i den mån de data som skyddas som företagshemligheter identifieras i avtalet.

Se klausul 5.1.2.

3. **Under avtalets giltighetstid** – Datahållarnas rättigheter avseende företagshemligheter kan dock också vara tillämpliga under avtalets giltighetstid, när det gäller nya data som ska göras tillgängliga.

Se klausul 5.1.3.

4. **Revisionsrättigheter** – För att bevara konfidentialiteten för de data som skyddas som företagshemligheter, utan att påverka varandras verksamhet, kan vissa revisionsrättigheter genom involvering av oberoende tredje parter övervägas, inklusive mekanismer i händelse av oenighet om resultaten i revisionsrapporten. Parterna kan använda alternativa åtgärder till revisioner.

Se klausul 5.2.3.

5. **Rättigheter för innehavare av företagshemligheter (1/4)** – Datahållaren (eller tredje part som är innehavare av företagshemligheter) kan komma överens med användaren om krav för att bevara konfidentialiteten för företagshemligheterna som ett villkor för att dela dessa identifierade företagshemligheter, till exempel att vidta vissa proportionerliga tekniska och organisatoriska åtgärder.

Se klausulerna 5.2 och 5.3.

6. **Rättigheter för innehavare av företagshemligheter (2/4)** – Om de initiala åtgärderna inte är tillräckliga kan innehavaren av företagshemligheter, från fall till fall, för specifika och identifierade data som skyddas som företagshemligheter, antingen ensidigt öka nivån på åtgärderna eller begära att användaren godkänner ytterligare åtgärder. Om det inte finns någon överenskommelse om nödvändiga åtgärder kan datahållaren, enligt villkoren i dataförordningen, avbryta delningen av specifika data som skyddas som företagshemligheter.

Se klausul 5.4.1.

7. **Rättigheter för innehavare av företagshemligheter (3/4)** – Innehavaren av företagshemligheter kan också, från fall till fall, vägra att dela specifika, identifierade företagshemligheter, enbart under exceptionella omständigheter och enligt de villkor som anges i dataförordningen.

Se klausul 5.4.2.

8. **Rättigheter för innehavare av företagshemligheter (4/4)** – Innehavaren av företagshemligheter kan hålla inne eller avbryta datadelningen om användaren bryter mot sina skyldigheter avseende skyddet av företagshemligheter.

Se klausul 5.4.3.

9. **Lagring av data som innehåller identifierade företagshemligheter** – Om datahållaren håller inne eller avbryter datadelningen i enlighet med klausulerna 5.4.1, 5.4.2 eller 5.4.3, är datahållaren fortfarande skyldig att hålla de relaterade data som innehåller identifierade företagshemligheter tillgängliga genom att lagra dem tills de kan delas inom ramen för avtalet.

Se klausul 5.6.

10. **Tredje part som är innehavare av identifierade företagshemligheter** – Om innehavaren av företagshemligheter är en tredje part måste datahållaren se till att klausul 5 också skyddar dennes företagshemligheter och inhämta alla relevanta tillstånd från nämnda tredje part som är innehavare av företagshemligheter.

Se klausul 5.1.2.

5.1. **Tillämplighet av avtal om företagshemligheter**

5.1.1. De skyddsåtgärder som avtalats i klausulerna 5.2 och 5.3 i detta avtal, samt de tillhörande rättigheter som avtalats i klausul 5.4, gäller uteslutande för data eller metadata som ingår i de data som datahållaren ska göra tillgängliga för användaren och som skyddas som företagshemligheter (enligt definitionen i direktivet om företagshemligheter) och som innehas av datahållaren eller en annan innehavare av företagshemligheter (enligt definitionen i det direktivet).

5.1.2. Identifieringen av data som skyddas som företagshemligheter och identiteten på innehavaren eller innehavarna av företagshemligheter anges i tillägg 4.

Datahållaren försäkrar användaren att denne har alla relevanta rättigheter från tredje part som innehar företagshemligheter för att ingå detta avtal avseende data som skyddas som företagshemligheter.

I enlighet med artikel 4.6 i dataförordningen ska ”datahållaren eller, om det inte rör sig om samma person, innehavaren av en företagshemlighet identifiera de data som skyddas som företagshemligheter, inbegripet relevanta metadata”.

Datahållaren bör därför identifiera de data som skyddas som företagshemligheter i **tillägg 4**. Datahållaren bör dock inte vara skyldig att beskriva själva företagshemligheten. Det räcker att identifiera de data som måste skyddas för att säkerställa konfidentialiteten för företagshemligheten, om analysen av sådana data skulle kunna röja företagshemligheten.

5.1.3. Om nya data som skyddas som företagshemligheter enligt punkt 5.1.1 under detta avtals giltighetstid görs tillgängliga för användaren, ska tillägg 4 ändras i enlighet med detta på begäran av datahållaren.

Tills dess att **tillägg 4** har ändrats och godkänts av parterna får datahållaren hålla inne eller tillfälligt avbryta delningen av de nya data som skyddas som företagshemligheter. I sådant fall ska datahållarens beslut vederbörligen motiveras och lämnas skriftligen till användaren utan oskäligt dröjsmål. Datahållaren ska också underrätta den behöriga myndighet som utsetts enligt artikel 37 i förordning (EU) 2023/2854 om att den har hållit inne eller avbrutit datadelningen och ange vilka åtgärder som inte har överenskommits eller genomförts.

5.1.4. De skyldigheter som anges i klausulerna 5.2 och 5.3 förblir i kraft efter avtalets upphörande, om inte parterna kommer överens om något annat.

5.2. **Skyddsåtgärder som vidtas av användaren**

5.2.1. Användaren måste tillämpa de skyddsåtgärder som anges i **tillägg 4** (*användarens skyddsåtgärder*).

Parterna bör i ett separat tillägg ange alla detaljer om dessa åtgärder, inklusive för situationer när användaren delar data med tredje part. Åtgärderna kan vara både tekniska (t.ex. kryptering, brandväggar, delad lagring osv.) och organisatoriska (t.ex. intern styrning, lämplig identitetshantering och åtkomstkontroller, involvering av en betrodd tredje part, sekretessavtal).

Eftersom åtgärderna måste vara proportionerliga, kommer deras innehåll att variera beroende på vilken typ av företagshemligheter det rör sig om. Åtgärderna kommer också att bero på om i) åtkomst ska ges till den plats där data lagras eller ii) data ska överföras i sin helhet till användaren. I det första fallet har datahållaren en högre grad av kontroll och kan själv tillämpa en del av skyddsåtgärderna, medan användaren kan ha en lägre användningsnivå för dessa data. I vilket fall som helst måste båda parterna fokusera på att uppnå dataförordningens avsedda verkningar. Därför måste de olika intressena balanseras utan att de avsedda verkningarna undergrävs.

5.2.2. Om användaren får göra data tillgängliga för en tredje part, kan användaren dela data som skyddas som företagshemligheter om

(a) användaren i) utan oskäligt dröjsmål informerar datahållaren om att data som skyddas som företagshemligheter kommer att göras tillgängliga för en tredje part, ii) anger vilka data det rör sig om och iii) uppger den tredje partens identitet, etableringsort och kontaktuppgifter för datahållaren,

(b) den tredje parten tillämpar de skyddsåtgärder som anges i tillägg 4.

5.2.3. [ALTERNATIV] [För att kontrollera om och i vilken utsträckning användaren har genomfört och upprätthåller användarens skyddsåtgärder, använder sig användaren antingen i) årligen, på användarens bekostnad, av en oberoende tredje part som användaren valt för att utföra en revisionsrapport om säkerhetsöverensstämmelse, eller ii) årligen, på datahållarens bekostnad, av en oberoende tredje part som datahållaren valt för att utföra en revisionsrapport om säkerhetsöverensstämmelse, förutsatt att denna oberoende tredje part har undertecknat ett sekretessavtal som tillhandahålls av användaren. Sådana säkerhetsrevisionsrapporter måste visa att användaren uppfyller klausul 5 och tillägg 4 som gäller vid den tidpunkten. Resultaten av revisionsrapporterna ska utan oskäligt dröjsmål lämnas till båda parterna.

Användaren kan välja mellan i) och ii). Om en part anser att säkerhetsrevisionsrapporten som erhållits på den andra partens bekostnad är felaktig, behåller den rätten att på egen bekostnad erhålla en säkerhetsrevisionsrapport från en annan oberoende tredje part. Om denna rätt utövas, kommer båda oberoende tredjepartsrevisorerna tillsammans med parterna att diskutera eventuella skillnader mellan de två rapporterna och sträva efter att lösa eventuella olösta frågor i god tro.

Denna klausul är markerad som ett alternativ, eftersom parterna kan komma överens om andra åtgärder för att kontrollera att användaren fullgör sina skyldigheter att genomföra och upprätthålla användarens skyddsåtgärder.

5.3. **Skyddsåtgärder som vidtas av innehavaren av företagshemligheter**

5.3.1. Datahållaren får tillämpa de åtgärder som överenskommits i **tillägg 4** för att bevara konfidentialiteten för de data som skyddas som företagshemligheter (nedan kallade *datahållarens skyddsåtgärder*).

5.3.2. Datahållaren får ensidigt vidta lämpliga tekniska och organisatoriska skyddsåtgärder, såsom uppdatering av programvara, om dessa inte påverkar användaren negativt enligt detta avtal.

5.3.3. Användaren förbinder sig att inte ändra eller ta bort datahållarens skyddsåtgärder eller de åtgärder som vidtagits i enlighet med klausul 5.3.2, om inte parterna kommit överens om annat.

5.4. **Skyldighet att dela och rätt att vägra, hålla inne eller säga upp**

5.4.1. Om den identifierade användarens skyddsåtgärder och datahållarens skyddsåtgärder inte är tillräckliga för att på ett adekvat sätt skydda en viss uppgift som skyddas som företagshemlighet, kan datahållaren, genom att meddela användaren med en detaljerad beskrivning av åtgärdernas otillräcklighet, begära att ytterligare skyddsåtgärder ska överenskommas. Om det efter en rimlig tidsperiod inte finns någon överenskommelse om nödvändiga ytterligare åtgärder och om behovet av sådana åtgärder är vederbörligen motiverat, t.ex. i en säkerhetsrevisionsrapport, kan datahållaren hålla inne eller avbryta delningen av de specifika data som avses. I sådant fall måste datahållaren meddela användaren. Meddelandet måste vara vederbörligen motiverat, ange vilka åtgärder som inte har överenskommits, i förekommande fall vilka företagshemligheter som berörs, och lämnas skriftligen utan oskäligt dröjsmål. Datahållaren måste fortsätta att dela alla data som skyddas som företagshemligheter utom dessa specifika data.

5.4.2. Om det under exceptionella omständigheter är mycket sannolikt att datahållaren kommer att lida allvarlig ekonomisk skada av att vissa data som skyddas som företagshemlighet lämnas ut till användaren trots att användarens skyddsåtgärder och datahållarens skyddsåtgärder har genomförts, får datahållaren vägra att dela eller avbryta delningen av de specifika data som avses.

Datahållaren måste utan oskäligt dröjsmål lämna ett vederbörligen motiverat meddelande till användaren och till den behöriga myndighet som utsetts enligt artikel 37 i dataförordningen.

Datahållaren måste dock fortsätta att dela alla data som skyddas som företagshemligheter utom dessa specifika data.

Vägran eller avbrytande av datadelning enligt artikel 4 i förordning (EU) 2023/2854 är endast tillåtet under exceptionella omständigheter. Meddelandet måste därför vara vederbörligen motiverat. Aspekter som kan beaktas är till exempel bristen på verkställbarhet av skyddet av företagshemligheter i länder utanför EU, arten och graden av konfidentialitet för den aktuella företagshemligheten eller den relevanta uppkopplade produktens unika och nya karaktär.

5.4.3. Om användaren underlåter att genomföra och upprätthålla sina skyddsåtgärder, och om denna underlåtenhet är vederbörligen motiverad av datahållaren, t.ex. i en säkerhetsrevisionsrapport, har datahållaren rätt att hålla inne eller avbryta delningen av de specifika identifierade företagshemligheterna tills användaren har löst incidenten.

I detta fall måste datahållaren utan oskäligt dröjsmål skriftligen lämna ett vederbörligen motiverat meddelande till användaren och till den behöriga myndighet som utsetts enligt artikel 37 i dataförordningen.

5.4.4. Klausul 5.4.1 ger inte datahållaren rätt att säga upp detta avtal.

Klausulerna 5.4.2 eller 5.4.3 ger datahållaren rätt att säga upp detta avtal endast med avseende på de specifika identifierade företagshemligheterna, och om

(a) samtliga villkor i klausul 5.4.2 eller klausul 5.4.3 har uppfyllts,

(b) parterna inte har nått någon lösning efter en rimlig tidsperiod, trots försök att nå en uppgörelse i godo, inklusive efter ingripande av den behöriga myndighet som utsetts enligt artikel 37 i dataförordningen, och

(c) användaren inte har fått ett domstolsbeslut av en behörig domstol som förpliktar datahållaren att göra data tillgängliga och det inte finns något pågående domstolsförfarande för ett sådant beslut.

5.5. **Avslutande av produktion och förstörelse av varor som innebär intrång**

Utan att det påverkar andra rättsmedel som är tillgängliga för datahållaren i enlighet med detta avtal eller tillämplig lag, kan datahållaren, om användaren ändrar eller tar bort tekniska skyddsåtgärder som datahållaren har vidtagit eller inte upprätthåller de tekniska och organisatoriska åtgärder som vidtagits i överenskommelse med datahållaren i enlighet med klausulerna 5.2 och 5.3, begära att användaren

(a) raderar de data som tillhandahållits av datahållaren och eventuella kopior av dessa, och/eller

(b) upphör med produktion, erbjudande eller utsläppande på marknaden eller användning av varor, härledda data eller tjänster som producerats på grundval av kunskap som erhållits genom de identifierade företagshemligheterna, eller import, export eller lagring av varor som innebär intrång för dessa ändamål, och förstöra alla varor som innebär intrång, om det finns en allvarlig risk för att den olagliga användningen av dessa data kommer att orsaka datahållaren eller innehavaren av en företagshemlighet betydande skada eller om en sådan åtgärd inte skulle vara oproportionerlig med hänsyn till intressena för datahållaren eller innehavaren av en företagshemlighet, och/eller

(c) ersätter den part som lider skada till följd av missbruk eller röjande av sådana data som olagligt erhållits eller använts.

5.6. **Lagring av data som skyddas som identifierade företagshemligheter**

5.6.1. Om datahållaren utövar sin rätt att vägra, hålla inne eller avbryta delningen av data med användaren i enlighet med klausulerna 5.4.1, 5.4.2 och 5.4.3, måste denne se till att de data som avses lagras så att de kan göras tillgängliga för användaren

(a) när lämpliga skyddsåtgärder har överenskommits och vidtagits, eller

(b) när en behörig myndighet eller domstol har fattat ett bindande beslut som kräver att datahållaren tillhandahåller dessa data till användaren.

Denna skyldighet att lagra data upphör när en behörig myndighet eller domstol i ett bindande beslut tillåter radering av dessa lagrade data eller när avtalet upphör att gälla.

5.6.2. Datahållaren ska stå för de kostnader som är nödvändiga för att lagra data enligt punkt 5.6.1. Användaren ska dock täcka sådana kostnader i den utsträckning som innehållandet eller avbrytandet av datadelning sker i enlighet med punkt 5.4.3.

6. **(om data görs tillgängliga av datahållaren på begäran av användaren) Användning av data av användaren**

6.1. **Tillåten användning och delning av data**

6.1.1. Användaren får använda de data som datahållaren tillhandahåller på begäran för alla lagliga ändamål och/eller, i den mån data överförs till eller kan hämtas av användaren, fritt dela data under förutsättning att de begränsningar som anges i klausul 6.2 iakttas.

6.2. **Begränsningar för användning och delning av data**

6.2.1. Användaren förbinder sig att inte göra följande:

(a) Använda data för att utveckla en uppkopplad produkt som konkurrerar med produkten, eller dela data med tredje part för detta ändamål.

(b) Använda sådana data för att få insikt i tillverkarens eller, i förekommande fall, datahållarens ekonomiska situation, tillgångar och produktionsmetoder.

(c) Använda tvångsmedel eller utnyttja luckor i datahållarens tekniska infrastruktur som är utformad för att skydda data i syfte att få åtkomst till data.

(d) Dela data med en tredje part som anses vara en grindvakt enligt artikel 3 i förordning (EU) 2022/1925.

6.2.2. [ALTERNATIV] [Utöver detta och i enlighet med artikel 4.2 i dataförordningen samtycker användaren och datahållaren till att begränsa eller förbjuda följande behandling (ange berörd behandling: åtkomst till, användning och/eller vidare delning av data), vilket skulle undergräva säkerhetskraven för produkten, såsom fastställs i unionsrätten (*ange berört rättsligt säkerhetskrav*), och därmed få allvarliga konsekvenser för fysiska personers hälsa, säkerhet eller trygghet.

Användaren förbinder sig att inte (ange relevanta begränsningar eller förbud relaterade till ovannämnda behandling).]

7. **Delning av data på användarens begäran med en datamottagare**

7.1. **Tillhandahållande av data till en datamottagare**

7.1.1. Data, tillsammans med relevanta metadata som är nödvändiga för att tolka och använda dessa data, måste tillhandahållas en datamottagare av datahållaren, utan kostnad för användaren, på begäran av användaren eller en part som agerar på dennes vägnar. Begäran kan göras med hjälp av det formulär som anges i **tillägg 3**, skickat till (*beskriv förfarandet för en enkel begäran via elektroniska medel där det är tekniskt genomförbart*). För att kontrollera att begäran görs av användaren ska datahållaren inte vara skyldig att lämna mer information än vad som är nödvändigt.

7.1.2. När användaren inte är den registrerade ska datahållaren endast göra personuppgifter tillgängliga för en tredje part efter begäran från användaren, när det finns en giltig rättslig grund för att göra personuppgifter tillgängliga enligt artikel 6 i förordning (EU) 2016/679 (allmänna dataskyddsförordningen) och endast när, i förekommande fall, de villkor som anges i artikel 9 i den förordningen och artikel 5.3 i direktiv 2002/58/EG (direktivet om integritet och elektronisk kommunikation) är uppfyllda.

I detta avseende måste användaren, när denne inte är den registrerade, i varje begäran som framställs enligt föregående klausul ange den rättsliga grunden för behandlingen enligt artikel 6 i förordning (EU) 2016/679 (och, i förekommande fall, det tillämpliga undantaget enligt artikel 9 i den förordningen och artikel 5.3 i direktiv 2002/58/EG) som ligger till grund för begäran om att personuppgifter ska göras tillgängliga.

7.1.3. Datahållaren måste göra data tillgängliga för en datamottagare, med data av minst samma kvalitet som när de blev tillgängliga för datahållaren, och i alla händelser i ett heltäckande, strukturerat, allmänt använt och maskinläsbart format, på ett enkelt och säkert sätt.

7.1.4. Om användaren lämnar in en sådan begäran ska datahållaren komma överens med datamottagaren om arrangemangen för att göra data tillgängliga i enlighet med kapitlen III och IV i dataförordningen.

7.1.5. Användaren erkänner att en begäran enligt klausul 7.1.1 inte kan gynna en tredje part som anses vara en grindvakt enligt artikel 3 i förordning (EU) 2022/1925 [ALTERNATIV] [och inte kan göras i samband med testning av nya uppkopplade produkter, ämnen eller processer som ännu inte har släppts ut på marknaden].

7.1.6. Användaren erkänner att tredje part endast får behandla de data som gjorts tillgängliga för denne enligt klausul 7.1.1 för de ändamål och på de villkor som överenskommits med användaren. Datahållaren kan inte hållas ansvarig gentemot användaren för att ett sådant avtal mellan användaren och tredje part saknas, såvida inte datahållaren kände till eller borde ha känt till denna brist.

8. **[ALTERNATIV om användaren är ett företag] Begränsningar av användarens rättigheter**

Användaren samtycker till (*ange syftet med, arten av och varaktigheten för begränsningen av användarens rätt att använda eller dela data och ange vilken del av data som berörs av sådana begränsningar*).

I enlighet med artikel 7.2 i dataförordningen ska ”[a]vtalsvillkor som till nackdel för användaren utesluter tillämpning av, avviker från eller ändrar verkan av användarens rättigheter enligt [kapitel II] inte vara bindande för användaren”.

Detta bör läsas mot bakgrund av skäl 25, där det anges att det inte ”hindrar […] att användare vid förbindelser mellan företag gör data tillgängliga för tredje parter eller datahållare enligt något lagligt avtalsvillkor, bland annat genom att samtycka till att begränsa eller inskränka vidare delning av sådana data, eller att de får proportionell ersättning, till exempel i utbyte mot att de avstår från sin rätt att använda eller dela sådana data”.

Sådana begränsningar är därför endast giltiga om de inte medför någon skada för användaren, vilket innebär att begränsningarna inte får skada användarens berättigade intressen.

Dessutom får denna klausul inte användas för att helt beröva användaren sina lagliga rättigheter enligt artiklarna 4 och 5 i dataförordningen, till exempel genom att användaren helt avstår från sin rätt att få åtkomst till data. Användaren kan endast samtycka till begränsningar av sina rättigheter om dessa är begränsade i omfattning och tid. Dessa får inte vara till nackdel för användaren. Detta kan till exempel vara specifika begränsningar av användningen av de data som har hämtats, eller innebära att man samtycker till att inte dela data vidare med en tredje part enligt skäl 25, eller att inte låta en datamottagare dela data vidare med en tredje part.

Denna klausul kan användas när användaren har ett intresse av sådana begränsningar, till exempel när datahållaren och användaren deltar i ett gemensamt industriprojekt.

Klausulen kan också tillämpas om användaren erhåller ersättning. Enbart mottagandet av ersättning är dock inte tillräckligt för att begränsningarna inte ska anses vara till nackdel för användaren. Ersättningen ska stå i proportion till begränsningarna.

Användaren kan efter eget gottfinnande godta eller avvisa begränsningarna enligt denna klausul.

9. **Ersättning till användaren**

9.1. **Ersättning**

Datahållaren åtar sig att ersätta användaren enligt vad som anges i detalj i **tillägg 7**, *(om tillämpligt)*, inklusive för begränsningar av användarens rättigheter i enlighet med klausul 8.

Parterna kan komma överens om ersättning för datahållarens användning och delning av data, närhelst de anser det vara rättvist och rimligt. De kan till exempel överväga sådan ersättning om datahållaren använder data för att utveckla nya produkter eller tjänster eller om datahållaren skapar aggregerade eller härledda data för kommersiella ändamål. Om data däremot används uteslutande för behoven i ett avtal som ingåtts med användaren eller för att säkerställa produktens eller den tillhörande tjänstens funktion, säkerhet och skydd, kan ersättning utebli.

Parterna bör dock vara medvetna om att om användaren till exempel begränsar sina rättigheter i enlighet med klausul 8, bör användaren ersättas, såsom förklaras i förklaringsrutan under klausul 8, och ersättningen bör stå i proportion till begränsningens omfattning.

På samma sätt kan ersättning behövas för att säkerställa en rättvis behandling av användaren, om användaren samtycker till att datahållaren får sälja data till tredje part i enlighet med klausul 3.2.1 a iii.

Om ersättning ska betalas måste parterna komma överens om dess art, som kan vara ekonomisk eller icke-ekonomisk.

9.2. **(tillämpligt för ekonomisk ersättning) Ränta vid försenad betalning**

Om betalningen av ersättningen försenas ska datahållaren betala användaren ränta på försenad ersättning från den tidpunkt då beloppet förfaller till betalning till den tidpunkt då betalningen sker, i enlighet med tillämplig lag.

10. **Överföring av användning och flera användare**

Den ursprungliga användaren kan permanent överföra äganderätten till produkten eller sin rätt att använda produkten till en efterföljande användare, till exempel när användaren säljer produkten (överföring av användning).

Den ursprungliga användaren kan också bevilja rättigheter att använda produkten och/eller ta emot tillhörande tjänster till ytterligare användare, samtidigt som den behåller sin roll som användare (flera användare), till exempel när

— ett företag hyr ut sin skåpbil till ett annat företag under vissa perioder av året, eller

— ett biluthyrningsföretag hyr ut sina bilar till kunder.

Datahållarens rätt att använda data

I sådana fall måste datahållaren ingå ett avtal med efterföljande eller ytterligare användare för att kunna använda data som genereras genom användningen av produkten eller tillhörande tjänster av sådana användare. Klausulerna nedan föreslår möjliga lösningar för ingående av ett sådant avtal, så att parterna kan välja den lösning som är mest anpassad till situationens specifika omständigheter.

Vid överföring kan parterna exempelvis komma överens om att den ursprungliga användaren underrättar datahållaren om överföringen, identiteten och kontaktuppgifterna för den efterföljande användaren, så att datahållaren kan kontakta den efterföljande användaren och ingå ett avtal med denne.

Vid flera användare kan en sådan lösning vara alltför betungande för datahållaren. Om den ursprungliga användaren kan agera på datahållarens vägnar är en möjlighet därför att den ursprungliga användaren inhämtar ytterligare användares samtycke till de villkor för åtkomst till och användning av data som anges i detta avtal.

I andra situationer kan det fortfarande vara möjligt och önskvärt för den ursprungliga användaren att meddela datahållaren kontaktuppgifterna för en ytterligare användare, så att datahållaren kan ingå ett avtal direkt med den ytterligare användaren.

Det är också möjligt att datahållaren inte behöver underrättas om en efterföljande eller ytterligare användare av den ursprungliga användaren för att ingå ett avtal, eftersom omständigheterna är sådana att de kan ingå ett avtal utan någon åtgärd från den ursprungliga användaren. Det kan till exempel hända att det krävs att ett konto som identifierar användaren skapas för att kunna använda produkten och/eller tillhörande tjänster. Om så är fallet kommer datahållaren att kunna ingå ett avtal med den efterföljande eller ytterligare användaren när de skapar sina egna konton. Detta kan dock kräva att den ursprungliga användaren säkerställer att den efterföljande eller ytterligare användaren inte använder deras konto.

Parternas åtkomsträttigheter i samband med överföring av användning och flera användare

Vid överföring av användning eller flera användare bör avtalet ge klarhet om vem som har åtkomst till data och under vilka villkor. Om ett företag (den ursprungliga användaren) till exempel hyr ut uppkopplade jordbruksmaskiner till enskilda jordbrukare (ytterligare användare) på dags- eller veckobasis, kan de data som genereras av jordbruksmaskinerna röja känslig företagsinformation om de enskilda jordbrukarna. Tillverkaren (datahållaren) kan inte utan vidare göra data enligt klausul 4 i detta avtal tillgängliga för den ursprungliga användaren (företaget som äger maskinerna) utan att först försäkra sig om att detta inte innebär ett intrång i enskilda jordbrukares (de ytterligare användarnas) konfidentiella information eller rättigheter.

De ytterligare eller efterföljande användarnas åtkomsträttigheter kan i synnerhet bero på en avtalsenlig kategorisering av data, till exempel:

— Användarens borttagbara data – Produkterna eller tillhörande tjänster gör det ofta möjligt för användaren att radera data som genereras under användningen. Vid överföring bör användaren radera sådana data. Annars kan sådana data vara tillgängliga för ytterligare eller efterföljande användare.

— Alltid borttagbara data – Data som datahållaren inte bör göra tillgängliga för ytterligare eller efterföljande användare.

— Kvarvarande data – Data som inte är användarens borttagbara eller alltid borttagbara data. Dessa data kan inte tas bort och omfattas inte av något sekretessavtal (dvs. data kommer även att vara tillgängliga för nya efterföljande användare). Sådana data kan inkludera data som måste vara tillgängliga för den ytterligare eller efterföljande användaren enligt lag eller i praktiken (till exempel i samband med uppdateringar som görs i ett uppkopplat fordon).

Datahållaren ska sortera data i dessa kategorier, särskilt i den information som avses i artikel 3.2 och 3.3 i dataförordningen, i detta avtal (till exempel i tillägg 1) eller i dokumentationen som rör produkten eller den tillhörande tjänsten.

Denna klausul 10 fokuserar på dataförordningen. Klausulen påverkar inte ytterligare lagstiftning, inklusive sektorslagstiftning, som kan reglera överföringen av en uppkopplad produkt eller tillhörande tjänst (t.ex. reprocessing av medicintekniska produkter).

10.1. **Överföring av användning**

Om användaren enligt avtal överför i) äganderätten till produkten, eller ii) sina tillfälliga rättigheter att använda produkten, och/eller iii) sina rättigheter att erhålla tillhörande tjänster till en efterföljande person (*efterföljande användare*) och förlorar sin status som användare efter överföringen, åtar sig parterna att följa kraven i denna klausul.

[ALTERNATIV 1] [Den ursprungliga användaren måste underrätta datahållaren om överföringen och tillhandahålla nödvändiga kontaktuppgifter för den efterföljande användaren, så att datahållaren kan ingå ett avtal med denne om datahållarens användning av data.]

[ALTERNATIV 2] [Datahållaren vidtar nödvändiga åtgärder för att ingå ett avtal med den efterföljande användaren om datahållarens användning av data. *(om tillämpligt)* Den ursprungliga användaren måste se till att den efterföljande användaren inte kan använda den ursprungliga användarens konto.]

Datahållarens rättigheter att använda produktdata eller data från tillhörande tjänster som genererats före överföringen påverkas inte av en överföring, dvs. de rättigheter och skyldigheter som rör de data som överförts enligt avtalet före överföringen fortsätter att gälla efter överföringen.

10.2. **Flera användare**

Om den ursprungliga användaren beviljar en annan part (*ytterligare användare*) rätt att använda produkten och/eller tillhörande tjänster samtidigt som denne behåller sin status som användare, förbinder sig parterna att följa kraven i denna klausul.

10.2.1. Den ytterligare användarens samtycke till datahållarens användning och delning av data

[ALTERNATIV 1] [I avtalet mellan den ursprungliga användaren och den ytterligare användaren inkluderar den ursprungliga användaren, på datahållarens vägnar, klausuler som i huvudsak återspeglar innehållet i detta avtal mellan den ursprungliga användaren och datahållaren, särskilt klausul 3 om datahållarens användning och delning av produktdata och/eller data från tillhörande tjänster, under den tid som produkten och/eller tillhörande tjänster används tillfälligt.]

[ALTERNATIV 2] [Den ursprungliga användaren underrättar datahållaren om förekomsten och varaktigheten av den ytterligare användarens rättigheter att använda produkten och/eller tillhörande tjänster samt dennes kontaktuppgifter, så att datahållaren kan ingå ett avtal med den ytterligare användaren om datahållarens användning och delning av dessa data.]

[ALTERNATIV 3] [Datahållaren vidtar nödvändiga åtgärder för att ingå ett avtal med den ytterligare användaren. *(om tillämpligt)* Den ursprungliga användaren måste se till att den ytterligare användaren inte kan använda den ursprungliga användarens konto.]

10.2.2. Dataåtkomst för den ytterligare användaren

[ALTERNATIV] [Den ursprungliga användaren fungerar som första kontaktpunkt för den ytterligare användaren, om den ytterligare användaren gör en begäran om dataåtkomst enligt artiklarna 4 eller 5 i dataförordningen. Datahållaren måste samarbeta med den ursprungliga användaren för att hantera begäran, enligt vad som anges i **tillägg 10**.]

10.3. **Den ursprungliga användarens ansvar**

I den mån den ursprungliga användarens underlåtenhet att fullgöra sina skyldigheter enligt klausulerna 10.1 och 10.2 leder till att datahållaren använder och delar produktdata eller data från tillhörande tjänster utan att det finns ett avtal med den efterföljande eller ytterligare användaren, ska den ursprungliga användaren ersätta datahållaren för eventuella skadeståndsanspråk från den efterföljande eller ytterligare användaren gentemot datahållaren för deras användning av data efter överföringen eller tillfällig användning av produkten och/eller tillhörande tjänster.

11. **Datum för tillämpning, avtalets löptid och uppsägning**

11.1. **Datum för tillämpning och löptid**

Detta avtal skulle normalt inte existera som ett fristående avtal, utan skulle ingås parallellt med avtalet om överlåtelse av äganderätten till produkten till användaren, vilket ger denne tillfälliga rättigheter att använda produkten och/eller med avtalet om en tillhörande tjänst.

Detta avtal måste i allmänhet förbli i kraft så länge som det andra avtalet tillåter användaren att använda produkten eller den tillhörande tjänsten. Likaså bör varken datahållaren eller användaren kunna säga upp detta avtal, utom i fall där den andra parten begår ett väsentligt avtalsbrott, eftersom detta annars skulle leda till en situation där användaren använder produkten och/eller den tillhörande tjänsten utan någon avtalsrättslig ram avseende rättigheter och skyldigheter enligt dataförordningen.

11.1.1. Detta avtal [ALTERNATIV 1] [träder i kraft omedelbart] [ALTERNATIV 2] [träder i kraft från och med den (*ange datum*)].

11.1.2. Avtalet ingås för [ALTERNATIV 1] [obestämd tid] [ALTERNATIV 2] [en fast period på (*ange*)], med förbehåll för eventuella skäl för upphörande eller uppsägning enligt detta avtal.

11.2. **Uppsägning**

Oavsett den avtalsperiod som avtalats enligt klausul 11.1 upphör detta avtal att gälla

(a) vid förstörelse av produkten eller permanent upphörande av den tillhörande tjänsten, eller när produkten eller den tillhörande tjänsten på ett oåterkalleligt sätt förlorar sin förmåga att generera data, eller

(b) när användaren förlorar äganderätten till produkten eller när användarens rättigheter avseende produkten enligt ett hyresavtal, leasingavtal eller liknande avtal eller användarens rättigheter avseende den tillhörande tjänsten upphör, eller

(c) när båda parter är överens om detta.

Leden b och c ska inte påverka avtalets fortsatta giltighet mellan datahållaren och eventuella efterföljande eller ytterligare användare.

11.3. **Verkningar av upphörande och uppsägning**

11.3.1. När avtalsperioden löper ut eller detta avtal sägs upp befrias båda parter från sin skyldighet att utföra och ta emot framtida prestationer, men detta påverkar inte de rättigheter och skyldigheter som har uppkommit fram till tidpunkten för uppsägningen.

Upphörande eller uppsägning påverkar inte de bestämmelser i detta avtal som ska gälla även efter avtalets upphörande, särskilt klausul 13.1 om konfidentialitet, klausul 13.4 om tillämplig lag och klausul 13.6 om tvistlösning.

11.3.2. Uppsägningen eller upphörandet av avtalet får följande verkningar:

(a) Datahållaren ska upphöra att hämta de data som genererats eller registrerats från och med dagen för uppsägningen eller upphörandet.

(b) Datahållaren har fortsatt rätt att använda och dela de data som genererats eller registrerats före dagen för uppsägningen eller upphörandet enligt vad som anges i detta avtal.

12. **Åtgärder vid avtalsbrott**

Parterna kan komma överens om att inte bara fastställa specifika rättigheter och skyldigheter avseende data (många av dessa redan följer av dataförordningen), utan även om allmänna avtalsrättsliga frågor, såsom en avtalsslutande parts rättigheter och åtgärder om den andra avtalsslutande parten inte fullgör sina skyldigheter.

För sådana allmänna avtalsrättsliga frågor kan parterna välja att förlita sig på lagstadgade standardregler eller andra avtalsmallar. Om de vill använda dessa standardavtalsvillkor bör de se till att dessa är förenliga med eventuell tvingande nationell rätt som kan vara tillämplig på avtalet.

12.1. **Fall av underlåtenhet att fullgöra sina skyldigheter**

12.1.1. En parts underlåtenhet att fullgöra en skyldighet är av grundläggande betydelse för detta avtal om

(a) underlåtenheten väsentligen berövar den andra parten det som den hade rätt att förvänta sig enligt detta avtal, såvida inte den part som underlåtit att fullgöra sina skyldigheter inte kunde förutse och rimligen inte kunde ha förutsett detta resultat, eller

(b) det av omständigheterna framgår att man i framtiden inte kan förlita sig på den part som underlåtit att fullgöra sina skyldigheter.

12.1.2. En parts underlåtenhet är ursäktlig om den beror på ett hinder utanför dess kontroll och den parten rimligen inte kunde förväntas ta hänsyn till hindret vid tidpunkten för ingåendet av detta avtal, eller undvika eller övervinna hindret eller dess konsekvenser.

Om hindret endast är tillfälligt gäller ursäkten under den period som hindret föreligger. Om förseningen dock innebär en grundläggande underlåtenhet att fullgöra sina skyldigheter, kan den andra parten behandla den som sådan.

Den part som underlåter att fullgöra sina skyldigheter måste se till att den andra parten utan oskäligt dröjsmål får kännedom om hindret och dess inverkan på partens förmåga att fullgöra sina skyldigheter, efter det att den part som underlåter att fullgöra sina skyldigheter har fått kännedom om eller rimligen kunde förväntas ha fått kännedom om dessa omständigheter. Den andra parten har rätt till skadestånd för ekonomisk skada som uppstår till följd av att ett sådant meddelande inte mottagits.

12.2. **Rättsmedel**

12.2.1. Om en part inte fullgör sina skyldigheter, ska den andra parten ha de rättsmedel som anges i följande klausuler, utan att det påverkar de rättsmedel som finns tillgängliga enligt tillämplig lag.

12.2.2. Rättsmedel som inte är sinsemellan oförenliga får kombineras.

12.2.3. En part får inte utnyttja ett rättsmedel i den mån det orsakar den andra partens underlåtenhet att fullgöra sina skyldigheter, till exempel om en brist i den egna datainfrastrukturen har gjort det omöjligt för den andra parten att fullgöra sina skyldigheter. En part får inte heller åberopa ett skadeståndsanspråk i den mån den kunde ha minskat skadan genom att vidta rimliga åtgärder.

12.2.4. Den skadelidande parten kan

(a) begära att den part som inte fullgör sina skyldigheter utan oskäligt dröjsmål fullgör sina skyldigheter enligt detta avtal, såvida detta inte är olagligt eller omöjligt eller om specifikt fullgörande skulle medföra kostnader för den part som inte fullgör sina skyldigheter som är oproportionerliga i förhållande till den fördel som den andra parten skulle erhålla,

(b) begära att den part som inte fullgör sina skyldigheter raderar data som har hämtats eller använts i strid med detta avtal och alla kopior därav,

(c) kräva skadestånd för ekonomisk skada som den andra parten har orsakat genom underlåtenhet att fullgöra sina skyldigheter och som inte är undantagen enligt klausul 12.1.2. Den part som underlåter att fullgöra sina skyldigheter är endast ansvarig för skador som den förutsåg eller rimligen kunde ha förutsett vid tidpunkten för ingåendet av detta avtal som ett resultat av sin underlåtenhet att fullgöra sina skyldigheter, såvida inte underlåtenheten var uppsåtlig eller grovt vårdslös.

12.2.5. Datahållaren kan också avbryta delningen av data med användaren tills användaren fullgör sina skyldigheter eller följer begränsningarna, genom att utan oskäligt dröjsmål lämna ett vederbörligen motiverat meddelande till användaren

a) om användarens underlåtenhet att fullgöra sina skyldigheter är grundläggande,

b) *(om tillämpligt)* förutsatt att samtliga andra villkor som anges i klausul 5.4.3 är uppfyllda, i de fall som beskrivs i klausul 5.4.3.

12.2.6. Användaren kan också

(a) upphäva det samtycke som getts till datahållaren enligt klausul 3 eller sitt samtycke till de begränsningar av användarens rättigheter som överenskommits enligt klausul 8, tills datahållaren fullgör sina skyldigheter, såvida detta inte skulle orsaka datahållaren en skada som är grovt oproportionerlig i förhållande till underlåtenheten eller dess verkningar,

(b) återkalla det tillstånd som getts till datahållaren enligt klausul 3 och/eller sitt samtycke till de begränsningar av användarens rättigheter som överenskommits enligt klausul 8, genom att meddela datahållaren, om

i) datahållarens underlåtenhet är grundläggande, eller

ii) i fall av underlåtenhet som inte är grundläggande, användaren har meddelat en rimlig tidsfrist för att avhjälpa underlåtenheten och tidsfristen har löpt ut utan att datahållaren har fullgjort sina skyldigheter. Den angivna tidsfristen anses vara rimlig om datahållaren inte invänder mot den utan oskäligt dröjsmål.

12.2.7. [ALTERNATIV] [Om en part underlåter att fullgöra sina skyldigheter enligt detta avtal ska den i alla fall betala de straffavgifter som anges i detalj i tillägg 8, vilka parterna anser vara skadestånd i den mening som avses i klausul 12.2.4 c. Den part som underlåter att fullgöra sina skyldigheter har rätt att begära att straffavgiften sänks till ett rimligt belopp om den kan bevisa att straffavgiften är grovt överdriven i förhållande till den skada som uppstått till följd av underlåtenheten.]

Parterna kanske vill fastställa påföljder för vissa typer av underlåtenhet, eftersom det kan vara alltför betungande för den skadelidande parten att bevisa storleken på den faktiska skada som orsakats av t.ex. underlåtenhet att tillhandahålla data. Påföljderna bör vara proportionerliga.

13. **Allmänna bestämmelser**

13.1. **Konfidentialitet**

13.1.1. Följande information ska betraktas som konfidentiell:

(a) Information som avser företagshemligheter, ekonomisk situation eller andra aspekter av en parts verksamhet, såvida inte den parten har offentliggjort denna information.

(b) Information som avser användaren och tredje part, såvida de inte redan har offentliggjort denna information.

13.1.2. Båda parterna samtycker till att vidta alla rimliga åtgärder för att lagra konfidentiell information på ett säkert sätt och att inte göra sådan information tillgänglig för tredje part, såvida inte

(a) en av parterna har en laglig skyldighet att göra relevant information tillgänglig,

(b) det är nödvändigt för en av parterna att göra relevant information tillgänglig för att fullgöra sina skyldigheter enligt detta avtal, eller

(c) en av parterna har erhållit förhandsgodkännande från den andra parten eller den part som tillhandahåller den konfidentiella informationen eller som påverkas av dess utlämnande.

13.1.3. Dessa skyldigheter avseende konfidentialitet gäller även efter avtalets upphörande under en period av (*ange period*).

13.1.4. Dessa skyldigheter avseende konfidentialitet upphäver inte strängare förpliktelser enligt i) förordning (EU) 2016/679 (allmänna dataskyddsförordningen), ii) bestämmelserna om genomförande av direktiv 2002/58/EG eller direktiv (EU) 2016/943, eller iii) annan unionsrätt eller nationell rätt, iv) (*om tillämpligt*) klausul 6 i detta avtal.

13.2. **Kommunikationsmedel**

Alla meddelanden eller annan kommunikation som krävs enligt detta avtal måste vara skriftliga och kan levereras personligen, skickas med förbetald post eller överföras elektroniskt, inklusive e-post, förutsatt att avsändaren behåller bevis på att de har skickats till nedanstående adresser:

Part	Kontaktperson	E-post	Telefon	Adress
Användare	[Namn]/[Befattning]	[E-post]	[Telefon]	[Adress]
Datamottagare	[Namn]/[Befattning]	[E-post]	[Telefon]	[Adress]

Sådana meddelanden eller kommunikationer ska anses ha mottagits

(a) om de levereras personligen, på leveransdagen,

(b) om de skickas med förbetald post, den tredje arbetsdagen efter att de postats,

(c) om de skickas elektroniskt, på överföringsdagen, förutsatt att avsändaren inte har mottagit något felmeddelande som indikerar att leveransen misslyckats.

13.3. **Hela avtalet, ändringar och avskiljbarhet**

13.3.1. Detta avtal (tillsammans med dess tillägg och andra dokument som hänvisas till i avtalet) utgör hela avtalet mellan parterna avseende avtalets innehåll och ersätter med avseende på innehållet alla muntliga eller skriftliga tidigare avtal, överenskommelser eller uppgörelser, mellan parterna.

13.3.2. Alla ändringar av detta avtal är endast giltiga om de har godkänts skriftligen, inklusive i elektronisk form.

13.3.3. Om någon bestämmelse i detta avtal av någon anledning befinns vara ogiltig, upphävbar eller icke verkställbar, och om denna bestämmelse kan särskiljas från övriga villkor i avtalet, ska de övriga bestämmelserna fortsätta att vara giltiga och verkställbara. Eventuella luckor eller oklarheter i detta avtal ska hanteras i enlighet med klausul 13.5.

13.4. **Tillämplig lag**

13.4.1. Detta avtal regleras av lagen i (*ange medlemsstat*).

13.5. **Tolkning**

13.5.1. Detta avtal ingås av parterna mot bakgrund av parternas rättigheter och skyldigheter enligt dataförordningen. Alla bestämmelser i detta avtal ska tolkas så att de överensstämmer med dataförordningen och annan unionsrätt eller nationell lagstiftning som antagits i enlighet med unionsrätten, samt all tillämplig nationell rätt som är förenlig med unionsrätten och som inte kan frångås genom avtal.

13.5.2. Om någon lucka eller oklarhet i detta avtal inte kan lösas på det sätt som anges i klausul 13.5.1, ska detta avtal tolkas mot bakgrund av de tolkningsregler som föreskrivs i tillämplig lag (se klausul 13.4).

13.6. **Tvistlösning**

13.6.1. Parterna är överens om att göra sitt yttersta för att lösa tvister i godo och, innan de väcker talan vid domstol, att hänskjuta tvisten till (*ange namn och kontaktuppgifter för ett särskilt tvistlösningsorgan; för tvister som omfattas av deras behörighet enligt artikel 10.1 i dataförordningen kan det vara vilket tvistlösningsorgan som helst i en medlemsstat som uppfyller villkoren i artikel 10 i dataförordningen*).

13.6.2. Överlämnande av en tvist till ett tvistlösningsorgan i enlighet med klausul 13.6.1 påverkar dock inte användarens rätt att lämna in ett klagomål till den nationella behöriga myndighet som utsetts i enlighet med artikel 37 i dataförordningen, eller någon parts rätt att söka ett effektivt rättsmedel vid en domstol i en medlemsstat.

13.6.3. [ALTERNATIV, om användaren är ett företag] [Domstolarna i (*ange medlemsstat*) har exklusiv behörighet att pröva mål som rör detta avtal.]

Tillägg 1

Detaljer om de data som omfattas av detta avtal och om villkoren för åtkomst

I detta tillägg ska parterna ange detaljer om de data som omfattas av detta avtal, om villkoren för åtkomst och om de medel och den information som krävs för att få åtkomst till och använda data, i enlighet med vad som anges i klausulerna 2 och 3.

A. **Specificering av datas innehåll**

I tillägget ska först de produktdata och data från tillhörande tjänster som omfattas av avtalet sorteras och listas, med angivande av innehållet i dessa data och insamlingsfrekvensen, så att användaren får precis information om innehållet i data (strukturerad förteckning över datapunkter eller exakta datakategorier).

B. **Lagringstid**

I tillägget ska sedan lagringstiden anges, så att användaren informeras om hur länge data är tillgängliga. Detta kan göras på ett detaljerat sätt för varje datapunkt eller grupp av datapunkter.

C. **Dataordning**

I tillägget ska anges om alla eller delar av data är särskilda data som regleras av en särskild ordning. I tillägget kan t.ex. anges huruvida och vilka data som kan betraktas som personuppgifter.

D. **Datastruktur och dataformat**

I tillägget ska anges i vilket strukturerat, allmänt använt och maskinläsbart format data görs tillgängliga.

E. **Åtkomstpolicy**

Det kan hända att användaren överför sina rättigheter att använda produkten eller att ta emot de tillhörande tjänsterna till en efterföljande användare eller att flera användare delar dessa rättigheter. I sådana fall ska parterna här ange åtkomsträttigheterna till data vid överföring av användningen av produkten eller vid flera användare. Tillägget kan särskilt ange följande:

— Användarens borttagbara data – Produkterna eller tillhörande tjänster gör det ofta möjligt för användaren att radera data som genereras under användningen. Vid överföring bör användaren radera sådana data. Annars kan sådana data vara tillgängliga för efterföljande användare.

— Alltid borttagbara data – Data som datahållaren inte bör göra tillgängliga för efterföljande användare.

— Kvarvarande data – Data som inte är användarens borttagbara eller alltid borttagbara data. Dessa data kan inte tas bort och omfattas inte av något sekretessavtal (dvs. data kommer även att vara tillgängliga för nya efterföljande användare). Sådana data kan inkludera data som måste vara tillgängliga för den efterföljande användaren enligt lag eller i praktiken (till exempel i samband med uppdateringar som görs i ett uppkopplat fordon).

F. **Överförings-/åtkomstmedium**

I tillägget bör anges vilket säkert och bekvämt elektroniskt medium som datahållaren kan använda för att göra data tillgängliga för användaren, antingen genom överföring eller åtkomst.

G. **Information som är nödvändig för att användaren ska kunna utöva sina åtkomsträttigheter**

I tillägget kan den information som är nödvändig för att användaren ska kunna utöva sina åtkomsträttigheter anges här. Informationen kan omfatta en kontaktperson som kan lösa tekniska problem, både hos datahållaren och hos användaren.

Tillägg 2

Innehåll i en begäran om åtkomst från användaren

Detta formulär är avsett för en enskild begäran. Flera begäranden är möjliga och rekommenderas till exempel för att segmentera vissa dataflöden så att dessa kan hanteras utifrån varje dataflöde, syfte och datalivscykel (till exempel personuppgiftsflöden och liknande).

Detta formulär innehåller de viktigaste delarna av en begäran, men dess form kan anpassas, särskilt för att passa elektroniska förfaranden.

Identifiering av användaren	Namn: Ange Avtal nr: *Ange*
Identifiering av den person som gör begäran på användarens vägnar (om tillämpligt)	Namn: Ange Relation till användaren: *Ange* Bifoga handlingar som styrker befogenheten att handla på användarens vägnar
Produkter och/eller tjänster som berörs av begäran	Produkt/tjänst 1: Ange (t.ex. serienummer) Produkt/tjänst 2: Ange (t.ex. serienummer)
Datapunkter som berörs av begäran	☐ Alla data som är lätt åtkomliga för datahållaren ☐ Övrigt: Ange de datapunkter som omfattas av begäran
Typ av begärda data	☐ Inklusive personuppgifter Om användaren inte är den registrerade, ange giltig rättslig grund för behandling enligt artikel 6 i förordning (EU) 2016/679 och, i förekommande fall, hur villkoren i artikel 9 i den förordningen och artikel 5.3 i direktiv 2002/58/EG är uppfyllda ☐ Endast icke-personuppgifter
Datum för de data som begäran avser	☐ Tidigare datum: Ange tidsperioden ☐ Kommande datum: Ange tidsperioden
Tidpunkt för dataåtkomst (beroende på vad som anges i tillägg 1)	☐ Kontinuerligt ☐ Realtid ☐ Övrigt: Ange
Sätt för dataåtkomst (beroende på vad som anges i tillägg 1)	☐ Överföring av data ☐ Åtkomst till data där de lagras
Destination för överföringen:	Ange beroende på svaret på föregående punkt
Datum för begäran	Ange

Tillägg 3

Formulär för begäran om åtkomst från användaren för att göra data tillgängliga för en tredje part

Detta formulär är avsett för en enskild begäran. Flera begäranden är möjliga och rekommenderas till exempel för att segmentera vissa dataflöden så att dessa kan hanteras av en viss datamottagare som utsetts av användaren från dataflöde till dataflöde och från syfte till syfte.

Identifiering av användaren	Namn: Ange Avtal nr: *Ange*
Identifiering av den person som gör begäran på användarens vägnar (om tillämpligt)	Namn: Ange Relation till användaren: *Ange*
Produkter och/eller tjänster som berörs av begäran	Produkt/tjänst 1: *Ange* Produkt/tjänst 2: *Ange*
Data som berörs av begäran Observera: gäller inte i samband med testning av nya uppkopplade produkter, ämnen eller processer som ännu inte har släppts ut på marknaden	☐ Alternativ 1: Alla data som är lätt åtkomliga för datahållaren ☐ Alternativ 2: Ange, i enlighet med tillägg 1 till avtalet mellan användaren och datamottagaren, vilka data som ska delas med datamottagaren ☐ Alternativ 3: Enligt vad som anges av datamottagaren i tillägg 2 till avtalet mellan datahållaren och datamottagaren
Om data innehåller personuppgifter	Ange giltig rättslig grund för behandling enligt artikel 6 i förordning (EU) 2016/679 och, i förekommande fall, hur villkoren i artikel 9 i den förordningen och artikel 5.3 i direktiv 2002/58/EG är uppfyllda
Identifiering av tredje part Observera: får inte vara en grindvakt enligt artikel 3 i förordning (EU) 2022/1925	Namn: Ange Kontaktuppgifter: *Ange*

Tillägg 4

Detaljer om åtgärder för skydd av företagshemligheter

(ska utarbetas av parterna)

[ALTERNATIV] Tillägg 5

Detaljer om delning av data med tredje part

(ska utarbetas av parterna)

Tillägg 6

Detaljer om skyddsåtgärder

(ska utarbetas av parterna)

[ALTERNATIV] Tillägg 7

Detaljer om ersättning till användaren

(ska utarbetas av parterna)

[ALTERNATIV] Tillägg 8

Detaljer om påföljder

(ska utarbetas av parterna)

[ALTERNATIV] Tillägg 9

Dokumentation om äganderätten till produkten eller avtalsenliga rättigheter att använda produkten eller tillhörande tjänster

(dokumentation ska bifogas av parterna)

[ALTERNATIV] Tillägg 10

Detaljer om villkor för ytterligare användares åtkomst till data

(ska utarbetas av parterna)

BILAGA III

STANDARDAVTALSVILLKOR

för avtal mellan användare och datamottagare

Dessa standardavtalsvillkor har utformats för avtal mellan en användare av en uppkopplad produkt och/eller tillhörande tjänst och en datamottagare med vilken användaren behöver eller vill dela sina data enligt artikel 5 i förordning (EU) 2023/2854 (nedan kallad *dataförordningen*).

Den viktigaste nyheten i dataförordningen i detta avseende är att

— användaren kan ålägga datahållaren att dela data med en datamottagare som användaren själv väljer,

— användaren i ett avtal med datamottagaren fastställer för vilka ändamål och på vilka villkor datamottagaren får använda och dela data,

— oskäliga avtalsvillkor om åtkomst till och användning av data, eller ansvar och rättsmedel vid överträdelse eller uppsägning av datarelaterade skyldigheter, inte är bindande om de har påtvingats ett företag ensidigt av ett annat företag.

Detta avtal följer ofta det avtal som ingås mellan datahållaren och användaren och föregår det avtal som också måste ingås mellan datahållaren och datamottagaren.

Detta avtal har en modulär struktur och kan användas som ett fristående avtal med alla klausuler (när datadelning är avtalets huvudsyfte), men parterna kan också välja specifika klausuler som passar deras specifika situation. Om datadelning endast var en förutsättning för fullgörandet av ett avtal som ingåtts för ett annat ändamål, t.ex. ett avtal om reparation och underhåll av en industrimaskin, kan det vara tillräckligt att använda klausulerna 1.2, 1.3, 2, 3 och 4 (med undantag för klausul 4.1.1 b), eftersom innehållet i de återstående klausulerna i detta avtal sannolikt skulle omfattas av reparations- och underhållsavtalet.

1. Parter och produkt/tillhörande tjänster

1.1. Avtalsparter

Detta avtal om åtkomst till och användning av data ingås mellan

(ange namn, kontaktuppgifter och ytterligare referenser) (*användaren*)

och

(ange namn, kontaktuppgifter och ytterligare referenser) (*datamottagaren*)

i detta avtal gemensamt benämnda *parterna* och var för sig *parten*.

Användare är en fysisk eller juridisk person som äger en uppkopplad produkt eller till vilken tillfälliga rättigheter att använda den uppkopplade produkten har överlåtits genom avtal, eller som erhåller tillhörande tjänster.

Datamottagare är en tredje part som användaren själv väljer. Det kan vara en fysisk eller juridisk person som agerar för syften kopplade till personens näringsverksamhet, affärsverksamhet, hantverk eller yrke och som är en annan än användaren av en uppkopplad produkt eller tillhörande tjänst, för vilken datahållaren gör data tillgängliga, inbegripet en tredje part på begäran från användaren till datahållaren eller i enlighet med en rättslig skyldighet enligt unionsrätten eller nationell lagstiftning som antagits i enlighet med unionsrätten.

En sådan datamottagare kan konkurrera med den berörda datahållaren. En grindvakt är dock inte berättigad att bli eller vara datamottagare.

1.2. Datamottagarens behörighet

Datamottagaren försäkrar att denne inte är utsedd till grindvakt enligt artikel 3 i förordning (EU) 2022/1925 ([1]) (*förordningen om digitala marknader*).

([1]) Europaparlamentets och rådets förordning (EU) 2022/1925 av den 14 september 2022 om öppna och rättvisa marknader inom den digitala sektorn och om ändring av direktiv (EU) 2019/1937 och (EU) 2020/1828 (förordningen om digitala marknader) (EUT L 265, 12.10.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/1925/oj).

1.3. **Begäran till datahållare och parternas samarbete**

1.3.1. Parterna är överens om att

[ALTERNATIV 1] [användaren begär att

(*ange namn, kontaktuppgifter och ytterligare referenser*) (*datahållaren*)

gör de data som anges i klausul 2 tillgängliga för datamottagaren.]

[ALTERNATIV 2] [användaren bemyndigar datamottagaren att på användarens vägnar begära att

(*ange namn, kontaktuppgifter och ytterligare referenser*) (*datahållaren*)

gör de data som anges i klausul 2 tillgängliga för datamottagaren.]

1.3.2. Användaren och datamottagaren ska samarbeta i god tro för att säkerställa adekvat kontakt och samarbete med datahållaren. Datamottagaren ska i synnerhet ingå ett separat avtal med datahållaren (*H2R-avtal*), [ALTERNATIV: i nära samråd med användaren] och i enlighet med tillämplig lagstiftning, inklusive men inte begränsat till dataförordningen. Datamottagaren måste säkerställa att H2R-avtalet överensstämmer med detta avtal.

1.3.3. Detta avtal ingås med avseende på

(a) följande uppkopplade produkt(er) (*produkten*): (*ange namn och ytterligare uppgifter om den specifika uppkopplade produkt som omfattas av avtalet*),

(b) följande tillhörande tjänst(er) (*tillhörande tjänst(er)*): (*ange namn och ytterligare uppgifter om de specifika tillhörande tjänster eller typ av tillhörande tjänster som omfattas av avtalet, om tillämpligt*).

Användaren försäkrar att han/hon antingen är ägare till produkten eller har avtalsenlig rätt att använda produkten enligt ett hyresavtal, leasingavtal eller liknande avtal och/eller att erhålla den/de relaterade tjänsten/tjänsterna enligt ett serviceavtal.

[ALTERNATIV 1] [Användaren förbinder sig att på vederbörligen motiverad begäran till datamottagaren tillhandahålla all relevant dokumentation som styrker denna förklaring, där så är nödvändigt.]

[ALTERNATIV 2] [Dokumentation som styrker denna förklaring samt uppgifter om vem som ska betraktas som användare enligt detta avtal anges i **tillägg 5**.]

2. **Data som omfattas av avtalet**

De data som omfattas av detta avtal består av alla lätt åtkomliga produktdata eller data från tillhörande tjänster som genereras genom användning av produkten eller de tillhörande tjänsterna:

[ALTERNATIV 1] [enligt definitionen i dataförordningen.]

[ALTERNATIV 2] [enligt definitionen i dataförordningen, som anges i tillägg 1.]

[ALTERNATIV 3] [enligt definitionen i dataförordningen, som är nödvändigt för de ändamål som överenskommits i klausul 3 och som vidare anges av datamottagaren i tillägg 2 till H2R-avtalet.]

Användaren ansvarar inte för datakvaliteten, egenskaperna och kvantiteten samt deras lämplighet för ett visst ändamål.

Enligt dataförordningen avses med ***produktdata*** ”data som genereras genom användning av en uppkopplad produkt och som tillverkaren har utformat för att kunna hämtas via en elektronisk kommunikationstjänst, via fysisk åtkomst eller åtkomst i enheten av en användare, datahållare eller en tredje part, inbegripet tillverkaren i tillämpliga fall”.

Med ***data från en tillhörande tjänst*** avses ”data som representerar digitaliseringen av användaråtgärder eller användarhändelser som kan härledas från den uppkopplade produkten och som registreras avsiktligt av användaren eller genereras som en biprodukt av användarens åtgärder under leverantörens tillhandahållande av en tillhörande tjänst”.

Produktdata och data från en tillhörande tjänst kan vara både personuppgifter och icke-personuppgifter.

Lätt åtkomliga data omfattar ”produktdata och data från en tillhörande tjänst som en datahållare lagligen erhåller eller lagligen kan erhålla från den uppkopplade produkten eller tillhörande tjänsten, utan oproportionella ansträngningar som går utöver en enkel åtgärd”.

Som förklaras i skälen omfattar denna definition inte ”data som genereras genom användning av en uppkopplad produkt om den uppkopplade produkten inte har utformats för att lagra eller överföra sådana data utanför den komponent i vilken de genereras eller den uppkopplade produkten som helhet” (skäl 20). ”Tillverkarnas val av utformning och, i förekommande fall, unionsrätt eller nationell rätt som tillgodoser sektorsspecifika behov samt mål eller relevanta beslut från behöriga myndigheter bör avgöra vilka data en uppkopplad produkt kan göra tillgängliga.” (skäl 14).

3. Datamottagarens användning av data

Avtal om datadelning mellan användare och datamottagare kan till exempel vara en ny relation eller ett tillägg till en befintlig relation mellan parterna, oavsett om det är för kommersiella datadelningsändamål eller inte. Sådana avtal bör vara icke-exklusiva, med undantag för fall som är väl avgränsade, dataspecifika, marknadsspecifika, ändamålsspecifika, tidsbegränsade och väl avlönade.

3.1. Överenskommen användning av data

Användaren avgör vilken del av dennes data och för vilket ändamål han eller hon tillåter datamottagaren att använda data, och i synnerhet i vilken utsträckning datamottagaren ska tillåtas att dela data med andra tredje parter.

Användaren kan till exempel be datamottagaren att övervaka produktens eller den tillhörande tjänstens funktion och agera som mellanhand som anmäler garantianspråk till säljaren av utrustningen på användarens vägnar.

Användaren bör också överväga om mottagaren ska tillåtas dela data med kommersiella eller icke-kommersiella enheter. Icke-kommersiell datadelning kan omfatta altruistisk eller annan icke-vinstdrivande delning och användning för allmännyttiga, vetenskapliga, statistiska eller andra analytiska forskningsändamål (där så är tillämpligt och krävs, eller inte är tillämpligt eller krävs men förutses i enlighet med artikel 89 i allmänna dataskyddsförordningen, direktivet om öppna data (EU) 2019/1024, förordningen om värdefulla dataset (EU) 2023/138, dataförvaltningsakten (EU) 2022/868, förordningen om hälsodataområden (EU) 2025/327 och liknande), av eller genom datamottagaren med relevanta samhällen, kommuner, regioner, nationer, icke-statliga organisationer och andra icke-kommersiella organisationer. För kommersiell datadelning rekommenderas att man inte hänvisar till eller använder termen *försäljning*, eftersom det för vissa intressenter kan innebära att rätten till/kontrollen över relevanta data överförs eller att sådana relevanta data på annat sätt överlämnas exklusivt till datamottagaren. Detta är varken nödvändigt eller rekommenderat, särskilt eftersom data både är en digital tillgång och ett digitalt medel och kan användas för många ändamål under hela sin livscykel – även för flera kommersiella ändamål – samtidigt som datamottagaren fortfarande får en marknadsfördel eller annat värdeskapande som också motiverar en skälig ersättning till användaren för att bevilja en sådan licens att (vidare)utnyttja dessa data.

Användaren bör bedöma konsekvenserna av att bevilja datamottagaren rätten att använda och, i förekommande fall, dela data, samt överväga om sådana rättigheter bör beviljas i utbyte mot ersättning.

3.1.1. Datamottagaren får endast använda data för följande ändamål, som inte får strida mot de metoder som anges i klausul 3.2: (*infoga överenskomna ändamål*).

Exempel på överenskomna ändamål för datamottagaren:

— Erbjuda regelbundet underhåll/eftermarknadstjänster för produkten till användaren.

— Bedriva forskning inom specifika områden.

— Utveckla nya tjänster eller förbättra, uppgradera eller upprätthålla nya produkter eller tjänster, inklusive lösningar för artificiell intelligens (AI).

— Aggregera data med andra data eller skapa härledda data för alla lagliga ändamål, inklusive i syfte att sälja eller på annat sätt göra sådana aggregerade eller härledda data tillgängliga för tredje part.

3.1.2. Datamottagaren måste radera data när de inte längre behövs för de överenskomna ändamålen.

3.2. **Obehörig användning av data**

Datamottagaren får inte använda data

(a) för något annat ändamål än de ändamål som överenskommits i klausul 3.1,

(b) för något ändamål som strider mot unionsrätten eller tillämplig nationell rätt,

(c) för profilering av fysiska personer i den mening som avses i artikel 4.4 i allmänna dataskyddsförordningen, såvida det inte är nödvändigt för att tillhandahålla den tjänst som användaren begärt,

(d) för att utveckla en produkt som konkurrerar med produkten,

(e) för att få insikter om användarens ekonomiska situation, tillgångar och produktionsmetoder, eller om användarens användning av produkten eller den tillhörande tjänsten på ett sätt som kan undergräva användarens kommersiella ställning på de marknader där användaren är verksam, såvida inte användaren har gett tillstånd till sådan användning,

(f) på ett sätt som negativt påverkar säkerheten för produkten eller någon tillhörande tjänst,

(g) [ALTERNATIV] [annat: *(ange, särskilt användningar som* avsevärt skadar användarens berättigade intressen)].

3.3. **Datamottagarens användning av personuppgifter**

Datamottagaren får endast använda eller på annat sätt behandla personuppgifter om det finns en rättslig grund för detta och endast på de villkor som fastställs i förordning (EU) 2016/679 (allmänna dataskyddsförordningen) och, i förekommande fall, direktiv 2002/58/EG (direktivet om integritet och elektronisk kommunikation).

Vid reglering av behandlingen av personuppgifter i enlighet med tillämplig dataskyddslagstiftning (inklusive men inte begränsat till förordning (EU) 2016/679) måste parterna överväga om användaren är den registrerade för samtliga eller delar av de personuppgifter som ingår i de data som omfattas.

3.4. **Tillämpning av skyddsåtgärder**

Datamottagaren åtar sig att tillämpa skyddsåtgärder för att förhindra förlust av data och obehörig åtkomst till data [ALTERNATIV 1] [som är rimliga under omständigheterna, med hänsyn till den vetenskapliga och tekniska utvecklingen, den potentiella skada som användaren kan drabbas av och kostnaderna för skyddsåtgärderna]. [ALTERNATIV 2] [som beskrivs i detalj i **tillägg 2**.]

Parterna bör överväga om de i ett separat tillägg vill inkludera alla detaljer om hur användarens viktiga intressen kan skyddas på ett effektivt sätt. Åtgärderna kan vara både tekniska (t.ex. kryptering, brandväggar, delad lagring) och organisatoriska (t.ex. involvering av en betrodd tredje part). Eftersom åtgärderna måste vara proportionerliga kommer deras innehåll att variera kraftigt beroende på vilken typ av data det rör sig om och vilka intressen som står på spel.

4. **Datadelning med tredje part och användning av databehandlingstjänster**

I enlighet med artikel 6.2 c i dataförordningen får datamottagaren inte ”göra de data som den tar emot tillgängliga för en annan tredje part, såvida inte datan görs tillgängliga på grundval av ett avtal med användaren, och förutsatt att den andra tredje parten vidtar alla nödvändiga åtgärder som överenskommits mellan datahållaren och den tredje parten för att bevara företagshemligheters konfidentialitet”.

Om användaren väljer att ge datamottagaren denna rättighet bör därför denna klausul införas, eventuellt mot ersättning.

4.1. **Villkor för datadelning**

4.1.1. Datamottagaren får dela data som inte är personuppgifter med tredje part om

(a) dessa används av tredje part uteslutande för att

i) hjälpa datamottagaren att uppnå de syften som överenskommits i klausul 3.1,

ii) i samarbete med datamottagaren eller genom företag med särskilt syfte uppnå de syften som överenskommits i klausul 3.1, och

iii) [ALTERNATIV] [(*ange de särskilda syften som tredje part kan eftersträva för sina egna behov, oberoende av datamottagaren, och om data delas för dessa syften mot ersättning eller gratis*), och]

(b) tredje parten inte är utsedd till grindvakt enligt artikel 3 i förordning (EU) 2022/1925 (*förordningen om digitala marknader*), och

(c) datamottagaren förbinder tredje part genom avtal

i) att inte använda data för något annat ändamål än de ändamål som överenskommits i klausul 4.1.1 a,

ii) att inte få insikter om användarens ekonomiska situation, tillgångar och produktionsmetoder, eller om användarens användning av produkten eller den tillhörande tjänsten på något annat sätt som kan undergräva användarens kommersiella ställning på de marknader där användaren är verksam,

iii) att inte använda data på ett sätt som avsevärt skadar användarens berättigade intressen, särskilt när sådana data är kommersiellt känsliga eller skyddas av företagshemligheter eller immateriella rättigheter,

iv) att tillämpa de skyddsåtgärder som krävs enligt klausul 3.4, och

v) att radera data när dessa inte längre är nödvändiga för de ändamål som överenskommits i klausul 4.1.1 a,

vi) att inte dela dessa data vidare.

4.1.2. Ytterligare detaljer, inklusive identiteten på tredje parter, begränsningar av tredje parters användning av data, samt ytterligare villkor och skyddsåtgärder, anges i detalj i **tillägg 3**.

4.1.3. Utan hinder av klausulerna 4.1.1 och 4.1.2 får datamottagaren använda behandlingstjänster, t.ex. molntjänster (inklusive infrastruktur som en tjänst, plattform som en tjänst och programvara som en tjänst), värdtjänster eller liknande tjänster för att för egen räkning och på eget ansvar uppnå de överenskomna syftena enligt klausul 3.2.1 a. Tredje parter får också använda sådana tjänster för att för egen räkning och på eget ansvar uppnå de överenskomna syftena enligt klausul 4.1.1 a. Datamottagaren får dela med tredje part eller på annat sätt behandla personuppgifter endast om det finns en rättslig grund och på de villkor som tillåts enligt förordning (EU) 2016/679 (allmänna dataskyddsförordningen) och, i förekommande fall, direktiv 2002/58/EG (direktivet om integritet och elektronisk kommunikation).

5. **Ersättning**

Datamottagaren åtar sig att ersätta användaren enligt vad som anges i detalj i **tillägg 4**.

Parterna kan komma överens om ersättning för datamottagarens användning och delning av data, närhelst de anser det vara rättvist och rimligt. De kan till exempel överväga sådan ersättning om datamottagaren använder data för att utveckla nya produkter eller tjänster eller om datamottagaren skapar aggregerade eller härledda data för kommersiella ändamål. Om dessa data däremot används uteslutande för behoven i ett avtal som ingåtts med användaren, kan ersättning komma att uteslutas.

På samma sätt kan ersättning behövas för att säkerställa en rättvis behandling av användaren, om användaren samtycker till att datamottagaren får sälja data till tredje part i enlighet med klausul 4.1.1 a iii. Om ersättning ska betalas måste parterna komma överens om dess art, som kan vara ekonomisk eller icke-ekonomisk.

6. **Datum för tillämpning, avtalets löptid och uppsägning**

6.1. **Datum för tillämpning och löptid**

6.1.1. Detta avtal [ALTERNATIV 1] [träder i kraft omedelbart] [ALTERNATIV 2] [träder i kraft från och med den (*ange datum*)].

6.1.2. [ALTERNATIV] [Detta avtal ingås för [ALTERNATIV 1] [obestämd tid] [ALTERNATIV 2] [en fast period på (*ange*)], med förbehåll för eventuella skäl för upphörande eller uppsägning enligt detta avtal.]

6.2. **Uppsägning**

6.2.1. Datamottagaren kan säga upp detta avtal genom att meddela användaren inom (*ange uppsägningstid*) om H2R-avtalet har sagts upp.

6.2.2. Om användaren förlorar sin status som användare upphör detta avtal. Användaren ska meddela datamottagaren inom (*ange uppsägningstid*).

6.2.3. [ALTERNATIV Vid obestämd löptid eller om parterna vill tillåta uppsägning av praktiska skäl] [Vardera parten kan säga upp detta avtal när som helst före avtalets början eller under avtalstiden genom att meddela den andra parten (*ange period*) i förväg.] [ALTERNATIV] Om användaren säger upp detta avtal enligt denna klausul före (*ange tidpunkt eller minsta avtalsperiod*), ska användaren ersätta den andra parten för de kostnader som uppkommit i samband med genomförandet av detta avtal enligt följande: (*ange tillämpligt alternativ*).

I fall där användaren enligt avtalet är skyldig att dela data med datamottagaren bör denna klausul inte inkluderas, eftersom det kan leda till brott mot ett annat avtal.

6.3. **Verkningar av upphörande eller uppsägning**

6.3.1. När avtalsperioden löper ut eller detta avtal sägs upp befrias båda parter från sin skyldighet att utföra och ta emot framtida prestationer, men detta påverkar inte de rättigheter och skyldigheter som har uppkommit fram till tidpunkten för upphörandet eller uppsägningen.

Upphörande eller uppsägning påverkar inte bestämmelser som ska gälla även efter det att avtalet har upphört, i synnerhet begränsningar av datamottagarens tillåtna användning och delning av data enligt klausulerna 3 och 4, klausul 8.1 om konfidentialitet, klausul 8.3 om tillämplig lag och klausul 8.6 om tvistlösning.

6.3.2. Uppsägningen eller upphörandet av avtalet får i synnerhet följande verkningar:

(a) Datamottagaren ska omedelbart upphöra att hämta de data som genererats eller registrerats från och med dagen för uppsägningen eller upphörandet.

(b) [ALTERNATIV] Datamottagaren har fortsatt rätt att använda och dela de data som genererats eller registrerats före dagen för uppsägningen eller upphörandet enligt klausulerna 3 och 4 [ALTERNATIV under en period av (*ange tid*)].

Det kan finnas fall där datamottagaren behöver investera i datadelning, till exempel genom att anpassa sin digitala infrastruktur. Investeringen kommer att amorteras över tid. I detta fall kanske parterna vill säkerställa att datamottagaren får ersättning från den uppsägande parten. Ersättningsbeloppet bör kunna fastställas.

7. Åtgärder vid underlåtenhet att fullgöra sina skyldigheter

7.1. Fall av underlåtenhet att fullgöra sina skyldigheter

7.1.1. En parts underlåtenhet att fullgöra en skyldighet är av grundläggande betydelse om

(a) underlåtenheten väsentligen berövar den andra parten det som den hade rätt att förvänta sig enligt detta avtal, såvida inte den part som underlåtit att fullgöra sina skyldigheter inte kunde förutse och rimligen inte kunde ha förutsett detta resultat, eller

(b) det av omständigheterna framgår att man i framtiden inte kan förlita sig på den part som underlåtit att fullgöra sina skyldigheter.

7.1.2. En parts underlåtenhet är ursäktlig om den beror på ett hinder utanför dess kontroll och den parten rimligen inte kunde förväntas ta hänsyn till hindret vid tidpunkten för ingåendet av detta avtal, eller undvika eller övervinna hindret eller dess konsekvenser.

7.1.3. Om hindret endast är tillfälligt ska underlåtenheten vara ursäktad för den period som hindret består. Om förseningen dock innebär en grundläggande underlåtenhet att fullgöra sina skyldigheter, kan den andra parten behandla den som sådan.

Den part som underlåter att fullgöra sina skyldigheter måste se till att den andra parten utan oskäligt dröjsmål får kännedom om hindret och dess inverkan på partens förmåga att fullgöra sina skyldigheter, efter det att den part som underlåter att fullgöra sina skyldigheter har fått kännedom om eller rimligen kunde förväntas ha fått kännedom om dessa omständigheter. Den andra parten har rätt till skadestånd för ekonomisk skada som uppstår till följd av att ett sådant meddelande inte mottagits.

7.2. Åtgärder vid underlåtenhet att fullgöra sina skyldigheter

7.2.1. Om en part inte fullgör sina skyldigheter, ska den andra parten ha de rättsmedel som anges i följande klausuler, utan att det påverkar de rättsmedel som finns tillgängliga enligt tillämplig lag.

7.2.2. Rättsmedel som inte är sinsemellan oförenliga får kombineras.

7.2.3. En part får inte utnyttja ett rättsmedel i den mån det är parten själv som orsakar den andra partens underlåtenhet att fullgöra sina skyldigheter, till exempel om en brist i den egna datainfrastrukturen har gjort det omöjligt för den andra parten att fullgöra sina skyldigheter. En part får inte heller åberopa ett skadeståndsanspråk i den mån den kunde ha minskat skadan genom att vidta rimliga åtgärder.

7.2.4. Den skadelidande parten kan

(a) säga upp detta avtal med omedelbar verkan utan påföljd genom att meddela den andra parten, om

i) den andra partens underlåtenhet att fullgöra sina skyldigheter är en grundläggande underlåtenhet, eller

ii) i fall av underlåtenhet som inte är grundläggande, den skadelidande parten har meddelat en rimlig tidsfrist för att avhjälpa underlåtenheten och tidsfristen har löpt ut utan att den andra parten har fullgjort sina skyldigheter,

(b) kräva skadestånd för ekonomisk skada som den andra parten har orsakat genom underlåtenhet att fullgöra sina skyldigheter och som inte är undantagen enligt klausul 7.1.2; den part som underlåter att fullgöra sina skyldigheter är endast ansvarig för skador som den förutsåg eller rimligen kunde ha förutsett vid tidpunkten för ingåendet av detta avtal som ett troligt resultat av sin underlåtenhet att fullgöra sina skyldigheter, såvida inte underlåtenheten var uppsåtlig eller grovt vårdslös,

(c) begära att den part som inte fullgör sina skyldigheter utan oskäligt dröjsmål fullgör sina skyldigheter enligt detta avtal, såvida detta inte är olagligt eller omöjligt eller om specifikt fullgörande skulle medföra kostnader för den part som inte fullgör sina skyldigheter som är oproportionerliga i förhållande till den fördel som den andra parten skulle erhålla, [ALTERNATIV] [om en part underlåter att fullgöra sina skyldigheter enligt detta avtal ska den i alla fall betala de straffavgifter som anges i detalj i tillägg 6, vilka parterna anser vara skadestånd i den mening som avses i klausul 7.2.4 b; den part som underlåter att fullgöra sina skyldigheter har rätt att begära att straffavgiften sänks till ett rimligt belopp om den kan bevisa att straffavgiften är grovt överdriven i förhållande till den skada som uppstått till följd av underlåtenheten.]

8. **Allmänna bestämmelser**

8.1. **Konfidentialitet**

8.1.1. Följande information ska betraktas som konfidentiell:

(a) Information som avser företagshemligheter, ekonomisk situation eller andra aspekter av den andra partens verksamhet, såvida inte den andra parten har offentliggjort denna information.

(b) (*om tillämpligt*) Information som anger grunden för beräkningen av ersättningen.

(c) Information som avser datahållaren och andra skyddade tredje parter, såvida inte den skyddade tredje parten har offentliggjort denna information.

8.1.2. Båda parterna är överens om att vidta alla rimliga åtgärder för att på ett säkert sätt lagra och behandla den information som avses i klausul 8.1.1 konfidentiellt och att inte lämna ut eller göra sådan information tillgänglig för tredje part, såvida inte

(a) en av parterna har en laglig skyldighet att lämna ut eller göra relevant information tillgänglig, eller

(b) det är nödvändigt för en av parterna att lämna ut eller göra relevant information tillgänglig för att fullgöra sina skyldigheter enligt detta avtal, eller

(c) en av parterna har erhållit förhandsgodkännande från den andra parten eller den part som tillhandahåller den konfidentiella informationen eller som påverkas av dess utlämnande.

8.1.3. Under alla omständigheter får användaren och datamottagaren lämna ut eller göra sådan information tillgänglig för datahållaren som är nödvändig för att identifiera eller kontakta datamottagaren eller användaren i syfte att ingå H2R-avtalet enligt klausul 1.3.2.

8.1.4. Dessa skyldigheter avseende konfidentialitet gäller även efter avtalets upphörande under en period av (*ange period*).

8.1.5. Dessa skyldigheter avseende konfidentialitet upphäver inte strängare förpliktelser enligt i) förordning (EU) 2016/679 (allmänna dataskyddsförordningen), ii) bestämmelserna om genomförande av direktiv 2002/58/EG eller direktiv (EU) 2016/943, eller iii) annan unionsrätt eller nationell rätt.

8.2. **Kommunikationsmedel**

Alla meddelanden eller annan kommunikation som krävs eller tillåts enligt detta avtal måste vara skriftliga och kan levereras personligen, skickas med förbetald post eller överföras elektroniskt, inklusive e-post, förutsatt att avsändaren behåller bevis på att de har skickats till nedanstående adresser:

Part	Kontaktperson	E-post	Telefon	Adress
Användare	[Namn]/[Befattning]	[E-post]	[Telefon]	[Adress]
Datamottagare	[Namn]/[Befattning]	[E-post]	[Telefon]	[Adress]

Sådana meddelanden eller kommunikationer ska anses ha mottagits

(a) om de levereras personligen, på leveransdagen,

(b) om de skickas med förbetald post, den tredje arbetsdagen efter att de postats,

(c) om de skickas elektroniskt, på överföringsdagen, förutsatt att avsändaren inte har mottagit något felmeddelande som indikerar att leveransen misslyckats.

8.3. **Hela avtalet, ändringar och avskiljbarhet**

8.3.1. Detta avtal (tillsammans med dess tillägg och andra dokument som hänvisas till i avtalet) utgör hela avtalet mellan parterna avseende avtalets innehåll och ersätter med avseende på innehållet alla tidigare muntliga eller skriftliga överenskommelser, avtal eller uppgörelser mellan parterna.

8.3.2. Alla ändringar av detta avtal är endast giltiga om de har godkänts skriftligen av parterna, inklusive i elektronisk form.

8.3.3. Om någon bestämmelse i detta avtal av någon anledning befinns vara ogiltig, upphävbar eller icke verkställbar, och om denna bestämmelse kan avskiljas från de återstående villkoren i avtalet, ska de övriga bestämmelserna inte påverkas av detta och fortsätta att vara giltiga och verkställbara, såvida inte bestämmelsen inte kan skiljas från övriga bestämmelser i detta avtal. Eventuella luckor eller oklarheter i detta avtal ska hanteras i enlighet med klausul 8.4.

8.4. **Tillämplig lag**

Detta avtal regleras av lagen i (*ange medlemsstat*).

8.5. **Tolkning**

8.5.1. Detta avtal ingås av parterna mot bakgrund av parternas rättigheter och skyldigheter enligt dataförordningen. Alla bestämmelser i detta avtal ska tolkas så att de överensstämmer med dataförordningen och annan unionsrätt eller nationell lagstiftning som antagits i enlighet med unionsrätten, samt all tillämplig nationell rätt som är förenlig med unionsrätten och som inte kan frångås genom avtal.

8.5.2. Om någon lucka eller oklarhet i detta avtal inte kan lösas på det sätt som anges i klausul 8.5.1, ska detta avtal tolkas mot bakgrund av de tolkningsregler som föreskrivs i tillämplig lag (se klausul 8.4).

8.6. **Tvistlösning**

8.6.1. Parterna är överens om att göra sitt yttersta för att lösa tvister i godo och, innan de väcker talan vid domstol, att hänskjuta tvisten till (*ange namn och kontaktuppgifter för ett särskilt tvistlösningsorgan; för tvister som omfattas av deras behörighet enligt artikel 10.1 i dataförordningen kan det vara vilket tvistlösningsorgan som helst i en medlemsstat som uppfyller villkoren i artikel 10 i dataförordningen*).

8.6.1. [ALTERNATIV, om användaren är ett företag] [Domstolarna i (*ange medlemsstat*) har exklusiv behörighet att pröva mål som rör detta avtal.]

Tillägg 1 innehåller en beskrivning av data

[ska utarbetas av parterna]

Tillägg 2 innehåller en förteckning över de skyddsåtgärder som datamottagaren ska vidta

[ska utarbetas av parterna]

Tillägg 3 innehåller information om datamottagarens delning av data med tredje part

[ska utarbetas av parterna]

Tillägg 4 innehåller information om ersättning till användaren för datamottagarens användning och delning av data

[ska utarbetas av parterna]

Tillägg 5 innehåller dokumentation om äganderätten till produkten eller avtalsenliga rättigheter att använda produkten eller tillhörande tjänster

[ska utarbetas av parterna]

[ALTERNATIV] **Tillägg 6** innehåller detaljer om påföljder

[ska utarbetas av parterna]

BILAGA IV

STANDARDAVTALSVILLKOR

för avtal mellan datahållare och datamottagare om att göra data tillgängliga på begäran av användare av uppkopplade produkter och tillhörande tjänster

Dessa standardavtalsvillkor har utformats för avtal mellan en datahållare och en datamottagare som är ett företag, där datahållaren är skyldig (enligt artikel 5 i förordning (EU) 2023/2854, nedan kallad *dataförordningen*) att göra data från en uppkopplad produkt och/eller tillhörande tjänst tillgänglig för en datamottagare när användaren begär detta.

Den viktigaste nyheten i dataförordningen i detta avseende är att

— datahållaren är skyldig att dela data med datamottagaren på begäran av användaren (med skyddsåtgärder för data som skyddas som företagshemligheter),

— datahållaren kan begära rimlig ersättning från datamottagaren,

— oskäliga avtalsvillkor om åtkomst till och användning av data, eller ansvar och rättsmedel vid överträdelse eller uppsägning av datarelaterade skyldigheter, inte är bindande om de har påtvingats ett företag ensidigt av ett annat företag.

Detta avtal har en modulär struktur och kan användas som ett fullständigt avtal, men parterna kan också välja vissa klausuler som passar deras specifika situation. Flera klausuler innehåller alternativ, och här bör parterna överväga sina specifika behov, affärsförbindelser och intressen för att identifiera det alternativ som bäst passar deras avtal.

Vissa klausuler är också markerade *(om tillämpligt)* och bör inkluderas om vissa villkor är uppfyllda.

Även om kommissionen rekommenderar standardavtalsvillkoren är de inte bindande och parterna kan alltid göra undantag från dem.
Villkoren kan också användas med lämpliga ändringar när en datahållare är skyldig att göra data tillgängliga för en tredjepartsdatamottagare enligt annan unionsrätt eller nationell rätt som antagits enligt unionsrätten.

1. Parter, begärande användare och produkt/tillhörande tjänst(er)

1.1. Avtalsparter

Detta avtal om åtkomst till och användning av data ingås

mellan

(*ange namn, kontaktuppgifter och ytterligare referenser*) (*datahållaren*)

och

(*ange namn, kontaktuppgifter och ytterligare referenser*) (*datamottagaren*)

i detta avtal gemensamt benämnda *parterna* och var för sig *parten*.

Parterna måste här ange vem som är datahållare och vem som är datamottagare, i den mening som avses i artikel 2.13 och 2.14 i dataförordningen.

Enligt dataförordningen avses med *datahållare* ”en fysisk eller juridisk person som har en rätt eller skyldighet, i enlighet med [dataförordningen], tillämplig unionsrätt eller nationell lagstiftning som antagits i enlighet med unionsrätten, att använda och tillgängliggöra data, inbegripet produktdata eller data från tillhörande tjänster som denne har hämtat eller genererat under tillhandahållandet av en tillhörande tjänst, om detta avtalats”.

Enligt dataförordningen avses med *datamottagare* ”en fysisk eller juridisk person som agerar för syften kopplade till personens näringsverksamhet, affärsverksamhet, hantverk eller yrke och som är en annan än användaren av en uppkopplad produkt eller tillhörande tjänst, för vilken datahållaren gör data tillgängliga, inbegripet en tredje part på begäran från användaren till datahållaren eller i enlighet med en rättslig skyldighet enligt unionsrätten eller nationell lagstiftning som antagits i enlighet med unionsrätten”. I enlighet med artikel 1.3 d i dataförordningen är datahållare endast skyldiga att göra data tillgängliga för ”datamottagare i unionen”. De är inte skyldiga att göra detta för datamottagare som är etablerade utanför unionen.

1.2. **Begärande användare, produkt/tillhörande tjänst(er)**

1.2.1. Detta avtal baseras på parternas gemensamma antagande att datahållaren enligt artikel 5 i dataförordningen är skyldig att göra data tillgängliga för datamottagaren när så begärs av eller på uppdrag av

(*ange namn, kontaktuppgifter och ytterligare referenser*) (*den begärande användaren*)

och att den begärande användaren är en användare (i den mening som avses i artikel 2.12 i dataförordningen) av

följande produkt: (*ange namn och ytterligare uppgifter om den specifika uppkopplade produkt eller typ av produkter som omfattas av avtalet*), och/eller

följande tillhörande tjänst(er): (*ange namn och ytterligare uppgifter om de specifika tillhörande tjänster eller typ av tillhörande tjänster som omfattas av avtalet, om tillämpligt*).

Parterna måste här ange vem som är användaren i den mening som avses i artikel 2.12 i dataförordningen, som gör en begäran till datahållaren enligt artikel 5 i .

Med ***användare*** avses en fysisk eller juridisk person som äger en uppkopplad produkt eller till vilken tillfälliga rättigheter att använda den uppkopplade produkten har överlåtits genom avtal, eller som erhåller tillhörande tjänster.

Parterna måste också ange vilken uppkopplad produkt och, i förekommande fall, vilken tillhörande tjänst som används av den begärande användaren.

Enligt dataförordningen avses med ***uppkopplad produkt*** en produkt
i) som erhåller, genererar eller samlar in data om sin användning eller om sin miljö,
ii) som kan kommunicera produktdata via en elektronisk kommunikationstjänst, fysisk åtkomst, åtkomst genom uppkoppling eller åtkomst i enheten,
iii) vars huvudfunktion inte är att lagra, behandla eller överföra data för någon annan part än användaren.

Med ***tillhörande tjänst*** avses en digital tjänst (annan än en elektronisk kommunikationstjänst, inbegripet programvara),
i) som är ansluten till produkten vid tidpunkten för köp, hyra eller leasing på ett sådant sätt att den uppkopplade produkten inte skulle kunna utföra en eller flera av sina funktioner utan den, eller
ii) som senare ansluts till produkten av tillverkaren eller en tredje part för att lägga till, uppdatera eller anpassa funktioner hos den uppkopplade produkten.

2. **Grunden för avtalet**

2.1. **Kvaliteten på den begärande användaren och förekomsten av en giltig begäran**

2.1.1. Varje part försäkrar att den begärande användaren, såvitt den vet, är en användare (enligt definitionen i artikel 2.12 i dataförordningen) av den produkt och de tillhörande tjänster som anges i klausul 1.2.1.

2.1.2. Varje part försäkrar att den begärande användaren har begärt att datahållaren gör de data som anges i klausul 3.1 tillgängliga för datamottagaren. Bevis på begäran bifogas detta avtal i **tillägg 1**.

2.1.3. *(Om tillämpligt)* Varje part försäkrar att den part som agerar på den begärande användarens vägnar, såvitt den vet, har fått nödvändig fullmakt från den begärande användaren att lämna in denna begäran i enlighet med tillämplig lag. Bevis på fullmakten bifogas detta avtal i **tillägg 1**.

Enligt dataförordningen kan begäran göras av en tredje part som agerar på den begärande användarens vägnar. Denna tredje part kan till exempel vara en dataförmedlare eller någon annan agent eller representant, inklusive datamottagaren själv.

Om en tredje part, inklusive datamottagaren, hävdar att den har fått fullmakt av den begärande användaren, är denna situation uppenbarligen en potentiell källa till missbruk jämfört med en vanlig begäran. Parterna måste därför vidta rimliga åtgärder för att säkerställa att det inte föreligger något bedrägeri eller någon manipulation och att denna begäran har lämnats in på korrekt sätt.

2.1.4. Varje part försäkrar att begäran, såvitt den vet, är giltig enligt tillämplig lag, inte har återkallats och inte har löpt ut.

Om det finns tecken på att begäran är ogiltig eller har återkallats måste parterna vidta rimliga åtgärder för att säkerställa att begäran fortfarande är giltig. Om så inte är fallet får datahållaren inte dela data med datamottagaren och kan hållas ansvarig för att ha gjort det. Datamottagaren kan också hållas ansvarig för att ha begärt data som denne inte har rätt att begära.

Begärans giltighet kan bero på många faktorer enligt tillämplig lag. För att en begäran ska vara juridiskt giltig kan det till exempel vara nödvändigt att den

— kan betraktas som en frivillig, tillräckligt informerad och uttrycklig indikation på den begärande användarens önskemål,

— lämnas med erforderlig rättskapacitet.

2.2. **Datamottagarens behörighet**

2.2.1. Datamottagaren försäkrar att det finns ett gällande avtal mellan denne och den begärande användaren som tillåter denne att använda data och att data enligt detta avtal kommer att användas uteslutande för (*ange syfte(n) enligt avtalet mellan datamottagaren och den begärande användaren*):

(*om data kan röja företagshemligheter*) Datamottagaren försäkrar att data är absolut nödvändiga för att uppfylla detta syfte.

I enlighet med artikel 6.1 i dataförordningen får datamottagaren endast använda data på grundval av ett avtal som ingåtts och för de ändamål som överenskommits med användaren. Datamottagaren ska här intyga att så är fallet. Om dessa uppgifter inte är eller inte längre är korrekta, kan datahållaren ha möjlighet att säga upp avtalet i enlighet med punkt 2.4.3.

Parterna bör sträva efter att fastställa de överenskomna ändamålen på ett sätt som gör det möjligt för datahållaren att avgöra om datamottagarens användning av data är tillåten, men inte så detaljerat att det röjer datamottagarens konfidentiella affärsidéer för datahållaren.

När det gäller datahållarens företagshemligheter måste de fullständiga syftena redovisas, så att datahållaren kan bedöma om tillhandahållandet av data är absolut nödvändigt för att uppnå det angivna syftet.

2.2.2. Datamottagaren försäkrar att denne inte är utsedd till grindvakt enligt artikel 3 i förordning (EU) 2022/1925 (*förordningen om digitala marknader*).

2.3. **Efterlevnad av dataskyddslagstiftningen**

2.3.1. I den mån data kan betraktas som personuppgifter försäkrar varje part att den följer förordning (EU) 2016/679 och, i förekommande fall, direktiv 2002/58/EG.

2.3.2. I synnerhet när den begärande användaren inte är den registrerade får datahållaren endast göra de data som är personuppgifter tillgängliga för datamottagaren i den utsträckning som tillåts enligt förordning (EU) 2016/679 och, i förekommande fall, direktiv 2002/58/EG.

Begreppet *personuppgifter* enligt dataskyddsförordningen är mycket brett. Det omfattar alla data som avser en identifierad eller identifierbar person, dvs. en fysisk person som kan identifieras, direkt eller indirekt, särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift, onlineidentifikation eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Icke-personuppgifter kan bli personuppgifter, till exempel när de ingår i en blandad datamängd, där de kombineras med nya data och resultatet av denna kombination gör det möjligt att koppla dessa data till en identifierad eller identifierbar person. Detta kan också inträffa när nya möjligheter till databehandling utvecklas.

Parterna bör börja med att noggrant bedöma förekomsten av personuppgifter i data samt sina egna roller och användarens roll enligt dataskyddsförordningen:

— *den registrerade*: den identifierade eller identifierbara fysiska person som uppgifterna avser.

— *personuppgiftsansvarig*: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter, om ändamålen och medlen för behandlingen bestäms av lag, kan den personuppgiftsansvarige föreskrivas i den lagen.

— *personuppgiftsbiträde*: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.

— *mottagare*: en fysisk eller juridisk person, offentlig myndighet, institution eller ett annat organ till vilket personuppgifterna utlämnas, vare sig det är en tredje part eller inte (med undantag för offentliga myndigheter som kan ta emot personuppgifter inom ramen för ett särskilt uppdrag enligt tillämplig lag).

Parterna bör beakta att en part kan ha mer än en roll beroende på ändamålet med behandlingen och/eller kan ha en roll tillsammans med en annan part.

En rättslig grund krävs enligt dataskyddsförordningen för att möjliggöra delning av data med datamottagaren. En möjlig rättslig grund för delning av personuppgifter där den begärande användaren inte är den registrerade kan vara samtycke från de berörda registrerade i den mening som avses i artikel 6.1 a eller berättigat intresse i den mening som avses i artikel 6.1 f i dataskyddsförordningen. För att bedöma förekomsten av ett sådant berättigat intresse kan skyldigheten att göra data tillgängliga i enlighet med artikel 5 i dataförordningen beaktas, även om denna skyldighet i sig inte är en tillräcklig rättslig grund.

2.4. **Felaktiga uppgifter**

2.4.1. En part som får kännedom om att någon av de uppgifter som avses i klausulerna 2.1–2.3 är eller inte längre är korrekta, eller inte längre kommer att vara korrekta inom överskådlig framtid, ska utan oskäligt dröjsmål underrätta den andra parten om detta, såvida inte den andra parten redan har eller borde ha kännedom om detta.

Om någon av de uppgifter som avses i punkterna 2.1–2.3 inte eller inte längre är korrekta, bör parten vidta lämpliga åtgärder. I synnerhet om den begärande användaren har sålt produkten och upphör att vara användare och datahållaren får lämplig information, bör datahållaren säga upp avtalet med datamottagaren avseende sådan användare. Datahållaren bör ange skälet till uppsägningen i uppsägningsmeddelandet. Enbart ett meddelande räcker inte i detta fall, eftersom det inte finns något sätt att rätta till situationen. Om datamottagaren vill fortsätta att ta emot data måste denne vända sig till den nya användaren. I vissa fall kan parterna dock rätta till representationen. Detta skulle till exempel vara fallet när användarens begäran utfärdas av en obehörig person (t.ex. en anställd som inte hade befogenhet att företräda användarens företag). I sådana fall kan tillämplig lag göra det möjligt att godkänna en sådan åtgärd med retroaktiv verkan.

2.4.2. När den berörda parten blir medveten om denna situation måste den vidta lämpliga åtgärder och i möjligaste mån rätta till felaktigheten i uppgifterna. Beroende på omständigheterna kan detta innefatta att underrätta den begärande användaren eller någon skyddad tredje part som berörs, eller att tillfälligt upphäva datahållarens tillhandahållande av data eller datamottagarens användning av data, om tillhandahållandet eller användningen av data har blivit olagligt.

2.4.3. Om situationen inte kan rättas till måste detta avtal sägas upp genom ett skriftligt uppsägningsmeddelande där den ena parten anger skälen för uppsägningen till den andra parten.

Uppsägningen träder i kraft omedelbart. Om felaktigheten endast påverkar en del av de data som omfattas av detta avtal, ska uppsägningen endast gälla den relevanta delen.

Verkningarna av uppsägningen regleras av klausul 7.3.

3. Tillhandahållande av data

3.1. Data som omfattas av avtalet

3.1.1. De data som omfattas av detta avtal består av lätt åtkomliga produktdata eller data från tillhörande tjänster i den mening som avses i dataförordningen, vilka identifierats i den begäran som den begärande användaren lämnat in i enlighet med artikel 5 i dataförordningen, och omfattar både icke-personuppgifter och personuppgifter (*data*).

De data som omfattas av avtalet anges i detalj i **tillägg 2**.

Om andra data än de som anges i **tillägg 2** måste göras tillgängliga för datamottagaren under avtalets giltighetstid, kommer **tillägg 2** att ändras i enlighet därmed.

Parterna ska i tillägg 2 ange de data och metadata som omfattas av avtalet, i enlighet med den begäran som den begärande användaren har gjort.

I enlighet med artiklarna 5 och 2.15, 2.16 och 2.17 i dataförordningen får dessa data endast vara lätt åtkomliga produktdata eller data från tillhörande tjänster:

— Produktdata är data som genereras genom användning av en produkt och som tillverkaren har utformat för att kunna hämtas via en elektronisk kommunikationstjänst, via fysisk åtkomst eller åtkomst i enheten av en användare, datahållare eller en tredje part, inbegripet tillverkaren i tillämpliga fall.

— Data från en tillhörande tjänst är data som representerar digitaliseringen av användaråtgärder eller användarhändelser som kan härledas från den uppkopplade produkten och som registreras avsiktligt av användaren eller genereras som en biprodukt av en användares åtgärder under tillhandahållandet av den tillhörande tjänsten.

— Lätt åtkomliga data är data som en datahållare lagligen kan erhålla från produkten eller tillhörande tjänsten, utan oproportionella ansträngningar som går utöver en enkel åtgärd.

Eftersom detta avtal fastställer villkoren för att göra data tillgängliga för datamottagaren på begäran av den begärande användaren, är dessa data de som anges i begäran.

Beskrivningen av data måste vara tillräcklig för att avgöra vilka data som omfattas av en särskild ordning, om sådan finns. Parterna bör särskilt ange vilka data som kan betraktas som personuppgifter.

3.2. Dataegenskaper och villkor för åtkomst

3.2.1. Datahållaren måste göra data tillgängliga för datamottagaren, med data av minst samma kvalitet som när de blev tillgängliga för datahållaren, och i alla händelser i ett heltäckande, strukturerat, allmänt använt och maskinläsbart format samt innehålla de relevanta metadata som är nödvändiga för att tolka och använda dessa data.

Med *metadata* avses en strukturerad beskrivning av innehållet i eller användningen av data som underlättar sökandet efter eller användningen av dessa data. I enlighet med artikel 5.1 i dataförordningen ska metadata göras tillgängliga tillsammans med data, i den mån metadata är ”nödvändiga för att tolka och använda” data.

Även om de relevanta metadata som behövs för att tolka och använda dessa data inte fastställs och därför måste identifieras från fall till fall, anges i dataförordningen att ”d[e] data som ska göras tillgängliga bör innefatta relevanta metadata, bland annat grundläggande information om sammanhang och tidsstämpel, för att göra datan användbar när den kombineras med andra data, såsom data sorterade och klassificerade med andra relaterade datapunkter, eller omformateras till ett allmänt använt format” (skäl 15 i dataförordningen).

3.2.2. Datamottagaren måste få åtkomst till data

a) enkelt och säkert,

b) utan oskäligt dröjsmål,

(om tillämpligt) c) kontinuerligt och i realtid.

3.2.3. För att uppfylla kraven i klausulerna 3.2.1 och 3.2.2 är parterna överens om de specifikationer som anges i tillägg 2.

I enlighet med artikel 5.1 i dataförordningen ska data göras tillgängliga utan oskäligt dröjsmål och, i tillämpliga fall och där så är tekniskt genomförbart, kontinuerligt och i realtid.

Eftersom det finns olika sätt att genomföra dessa rättsliga krav bör parterna komma överens om alla detaljer om hur åtkomst ska tillhandahållas i **tillägg 2**.

I detta sammanhang bör parterna som ett första steg besluta om de vill tillhandahålla

— **fullständig överföring** av data, dvs. en kopia av data överförs till ett medium som kontrolleras av datamottagaren

  — genom överföring som initieras av datahållaren (push), t.ex. onlineöverföring, uppladdning till datamottagarens molnutrymme eller leverans av ett fysiskt medium på vilket data lagras, eller

  — genom hämtning som initieras av datamottagaren (pull), t.ex. genom tillhandahållande av ett API, åtkomst till datahållarens molnutrymme eller liknande verktyg som gör det möjligt för datamottagaren att få åtkomst till och extrahera data, eller

— **åtkomst till data där de lagras**, dvs. data nås och behandlas på ett medium som kontrolleras av datahållaren eller en betrodd tredje part, t.ex. genom att datamottagaren loggar in på ett särskilt utrymme på datahållarens eller den betrodda tredje partens servrar, men data överförs inte till ett medium som kontrolleras av datamottagaren, såvida inte särskilda arrangemang har gjorts.

Fullständig överföring ger datamottagaren maximal frihet, men minskar avsevärt datahållarens möjlighet att förhindra missbruk.

Åtkomst till den plats där data lagras ökar risken för datamottagarna att deras affärsidéer blir kända, men ökar avsevärt datahållarens möjlighet att förhindra missbruk.

Utöver fullständig överföring och åtkomst till den plats där data lagras finns det ytterligare tekniska möjligheter, inklusive åtkomst på den begärande användarens enhet.

Om parterna väljer åtkomst till den plats där data lagras finns det ett antal frågor att lösa, bland annat hur man kan säkerställa att datamottagarens affärsidéer inte röjs och vilka data datamottagaren får överföra till ett medium som denne själv kontrollerar (t.ex. härledda eller avledda data som är resultatet av datamottagarens behandling).

Generellt sett får villkoren för åtkomst till den plats där data lagras inte undergräva några av de rättigheter som den begärande användaren eller datamottagaren har enligt dataförordningen eller annan tillämplig lagstiftning.

Åtkomst till de data som lagras på ett medium som kontrolleras av en betrodd tredje part är ofta att föredra framför åtkomst till ett medium som kontrolleras av datahållaren. Åtkomst till den plats där data lagras bör normalt fortfarande innebära fjärråtkomst, och åtkomst på plats bör begränsas till extrema situationer med högsta grad av känslighet.

Parterna måste också fastställa tidpunkten för åtkomst till data. I enlighet med artikel 5.1 i dataförordningen ska data, när användaren så begär, göras tillgängliga utan oskäligt dröjsmål och, i tillämpliga fall och där så är tekniskt genomförbart, kontinuerligt och i realtid.

Sådan åtkomst är dock inte alltid nödvändig för att uppnå de syften som datamottagaren och den begärande användaren har kommit överens om i ett specifikt fall. Parterna måste därför komma överens om frågor som rör tidpunkten för åtkomst till data, t.ex. om åtkomst ska ges i realtid, om det är relevant och tekniskt genomförbart, och om inte, med vilken frekvens.

Parterna måste också överväga en rad ytterligare frågor, såsom vilka behörigheter som krävs för åtkomst och vilka och hur många av datamottagarens anställda som får åtkomst till data.

3.2.4. Om data görs tillgängliga i enlighet med specifikationerna i tillägget om dataegenskaper och villkor för åtkomst, och om det framgår att de överenskomna specifikationerna är otillräckliga för att uppfylla kraven i klausulerna 3.2.1 och 3.2.2, åtar sig parterna att inleda förhandlingar i god tro och anpassa specifikationerna så att de uppfyller de överenskomna kraven.

3.2.5. Datahållaren måste tillhandahålla datamottagaren den information som är nödvändig för att få åtkomst till eller ta emot data i enlighet med artikel 5 i dataförordningen.

Detta innefattar särskilt tillhandahållande av information som är lätt åtkomlig för datahållaren om ursprunget till data och eventuella rättigheter som tredje part kan ha avseende dessa data, såsom rättigheter för registrerade som följer av förordning (EU) 2016/679 (allmänna dataskyddsförordningen), eller omständigheter som kan ge upphov till sådana rättigheter.

Datahållaren specificerar denna information i **tillägg 2**.

Parterna är fria att komma överens om ytterligare stöd, utöver kraven i dataförordningen, utan kostnad eller mot en avgift.

3.2.6. Datahållaren förbinder sig att inte lagra någon information om datamottagarens åtkomst till begärda data utöver vad som är nödvändigt för

(a) ett korrekt genomförande av i) den begärande användarens begäran om åtkomst och ii) detta avtal,

(b) säkerheten och underhållet av datainfrastrukturen, och

(c) fullgörandet av datahållarens lagliga skyldigheter att lagra sådan information.

3.3. **Återkoppling**

3.3.1. Om datamottagaren identifierar en incident som rör klausul 3.1 om de data som omfattas av avtalet eller klausul 3.2 om dataegenskaper och villkor för åtkomst, och om datamottagaren förser datahållaren med en detaljerad beskrivning av incidenten, måste datahållaren och datamottagaren samarbeta i god tro för att identifiera orsaken till incidenten. Om incidenten orsakades av att datahållaren inte fullgjort sina skyldigheter måste denne åtgärda överträdelsen utan oskäligt dröjsmål. Om datahållaren inte gör detta anses det vara en grundläggande underlåtenhet att fullgöra sina skyldigheter, och datamottagaren har rätt att åberopa klausul 8 i detta avtal (åtgärder vid avtalsbrott).

3.3.2. Om någon av de specifikationer som överenskommits i enlighet med klausul 3.2 är omöjlig eller alltför betungande att uppnå på grund av en exceptionell förändring av omständigheterna som inträffat efter avtalets ingående, måste datahållaren tillhandahålla datamottagaren en detaljerad beskrivning av detta och parterna ska inleda förhandlingar i god tro och anpassa specifikationerna så att de uppfyller kraven i dessa klausuler. I synnerhet måste varje part förse den andra med tillräcklig information för att bedöma, diskutera och lösa den specifika situationen. Denna klausul påverkar inte datamottagarens rätt att åberopa rättsmedel i enlighet med klausul 8.

3.4. **Ensidiga ändringar av datahållaren**

3.4.1. Datahållaren får ensidigt ändra detaljerna i specifikationerna för dataegenskaper och villkor för åtkomst, om detta är objektivt motiverat av datahållarens normala affärsverksamhet, till exempel genom en teknisk modifiering på grund av en omedelbar säkerhetsrisk i den produktlinje eller de tillhörande tjänster som datahållaren erbjuder eller en förändring i datahållarens infrastruktur. Alla ändringar måste uppfylla kraven i klausul 3.2.

3.4.2. Datahållaren måste meddela datamottagaren om ändringen minst (*ange en rimlig tidsperiod*) innan ändringen träder i kraft.

En kortare tidsfrist kan vara tillräcklig

(a) om ändringen inte påverkar datamottagarens åtkomst till och användning av data negativt, eller

(b) om ett sådant meddelande skulle vara omöjligt eller orimligt under omständigheterna, till exempel om omedelbara ändringar krävs på grund av en säkerhetsbrist som just har upptäckts.

3.4.3. Om ändringen påverkar datamottagarens åtkomst till och användning av data negativt, har datamottagaren rätt att säga upp (den relevanta delen av) avtalet utan att någon ersättning ska betalas till datahållaren, utan att detta påverkar datamottagarens eventuella andra rättigheter eller rättsmedel.

4. **(om data måste skyddas som företagshemligheter) Skydd av företagshemligheter**

1. **Delning av företagshemligheter** – Datahållare kan i princip inte avslå en begäran om åtkomst till data enligt dataförordningen enbart på grundval av att vissa data anses vara skyddade som företagshemligheter, eftersom detta skulle undergräva dataförordningens avsedda verkningar.

Se klausul 4.1.

2. **Företagshemligheter** – Om datahållaren dock fastställer att vissa data som omfattas av detta avtal är skyddade som företagshemligheter enligt definitionen i direktiv (EU) 2016/943[8] (nedan kallat *direktivet om företagshemligheter*) har datahållaren vissa rättigheter, främst rätten att fortsätta att bevara konfidentialiteten för de aktuella hemligheterna.

Enligt artikel 2.1 i direktivet om företagshemligheter avses med *företagshemlighet* information som uppfyller tre krav: a) Den är hemlig i den meningen att den inte, som helhet eller i den form dess beståndsdelar ordnats och satts samman, är allmänt känd hos eller lättillgänglig för personer i de kretsar som normalt sett handskas med typen av information i fråga. b) Den har kommersiellt värde på grund av att den är hemlig. c) Den person som lagligen kontrollerar den har med hänsyn till omständigheterna vidtagit rimliga åtgärder för att hålla den hemlig.

Med *innehavare av en företagshemlighet* avses en fysisk eller juridisk person som lagligen kontrollerar en företagshemlighet.

Data kan endast identifieras som företagshemligheter om de skyddas som sådana av datahållaren eller innehavaren av företagshemligheten när en begäran om åtkomst till data görs i enlighet med artikel 5 i dataförordningen.

Se klausul 4.1.1.

3. **Initial identifiering av företagshemligheter** – Datahållarnas rättigheter avseende företagshemligheter är – initialt – endast tillämpliga om och i den mån de data som skyddas som företagshemligheter identifieras i avtalet.

Se klausul 4.1.2.

4. **Under avtalets giltighetstid** – Datahållarnas rättigheter avseende företagshemligheter kan dock också vara tillämpliga under avtalets giltighetstid, när det gäller nya data som ska göras tillgängliga.

Se klausul 4.1.3.

5. **Revisionsrättigheter** – För att bevara konfidentialiteten för de data som skyddas som företagshemligheter ska vissa revisionsrättigheter genom involvering av oberoende tredje parter övervägas (utan att detta påverkar datahållarens eller datamottagarens verksamhet), inklusive mekanismer i händelse av oenighet om resultaten i revisionsrapporten.

Se klausul 4.2.3.

6. **Rättigheter för innehavare av företagshemligheter (1/4)** – Datahållaren (eller tredje part som är innehavare av företagshemligheter) kan komma överens med datamottagaren om krav för att bevara konfidentialiteten för företagshemligheterna som ett villkor för att dela dessa identifierade företagshemligheter, till exempel att vidta vissa proportionerliga tekniska och organisatoriska åtgärder.

Se klausulerna 4.2 och 4.3.

7. **Rättigheter för innehavare av företagshemligheter (2/4)** – Om de initiala åtgärderna inte är tillräckliga kan innehavaren av företagshemligheter, från fall till fall, för specifika och identifierade uppgifter som skyddas som företagshemligheter, antingen ensidigt öka nivån på åtgärderna eller begära att datamottagaren godkänner ytterligare åtgärder. Om det inte finns någon överenskommelse om nödvändiga åtgärder kan datahållaren, enligt villkoren i dataförordningen, avbryta delningen av specifika data som skyddas som företagshemligheter.

Se klausul 4.4.2.

8. **Rättigheter för innehavare av företagshemligheter (3/4)** – Innehavaren av företagshemligheter kan också, från fall till fall, vägra att dela specifika, identifierade företagshemligheter, enbart under exceptionella omständigheter och enligt de villkor som anges i dataförordningen.

Se klausul 4.4.3.

9. **Rättigheter för innehavare av företagshemligheter (4/4)** – Innehavaren av företagshemligheter kan hålla inne eller avbryta datadelningen om datamottagaren bryter mot sina skyldigheter avseende skyddet av företagshemligheter.

Se klausul 4.4.4.

10. **Lagring av data som innehåller identifierade företagshemligheter** – Om datahållaren håller inne eller avbryter datadelningen i enlighet med klausulerna 4.4.1, 4.4.2 eller 4.4.3, är datahållaren fortfarande skyldig att hålla de relaterade data som innehåller identifierade företagshemligheter tillgängliga genom att lagra dem tills de kan delas inom ramen för avtalet.

Se klausul 4.5.

11. **Tredje part som är innehavare av identifierade företagshemligheter** – Om innehavaren av företagshemligheter är en tredje part måste datahållaren se till att klausul 4 också skyddar deras företagshemligheter och inhämta alla relevanta tillstånd från nämnda tredje part som är innehavare av företagshemligheter.

Se klausul 4.1.2.

4.1. **Tillämplighet av avtal om företagshemligheter**

4.1.1. De skyddsåtgärder som avtalats i klausulerna 4.2 och 4.3 i detta avtal, samt de tillhörande rättigheter som avtalats i klausul 4.4, gäller uteslutande för data eller metadata som ingår i de data som datahållaren ska göra tillgängliga för datamottagaren och som skyddas som företagshemligheter (enligt definitionen i artikel 2.1 i direktivet om företagshemligheter) och som innehas av datahållaren eller en annan innehavare av företagshemligheter (enligt definitionen i artikel 2.2 i det direktivet).

4.1.2. Identifieringen av data som skyddas som företagshemligheter och identiteten på innehavaren av företagshemligheter anges i tillägg 4.

Datahållaren försäkrar datamottagaren att denne har alla relevanta rättigheter från tredje part som innehar företagshemligheter för att ingå detta avtal avseende data som skyddas som företagshemligheter.

I enlighet med artikel 5.9 i dataförordningen ska ”datahållaren eller, om det inte rör sig om samma person, innehavaren av en företagshemlighet identifiera de data som skyddas som företagshemligheter, inbegripet relevanta metadata”.
Datahållaren bör därför identifiera de data som skyddas som företagshemligheter i **tillägg 4**. Datahållaren bör dock inte vara skyldig att beskriva själva företagshemligheten. Det räcker att identifiera de data som måste skyddas för att säkerställa konfidentialiteten för företagshemligheten, eftersom analysen av sådana data skulle kunna röja företagshemligheten.

4.1.3. Om nya data som skyddas som företagshemligheter enligt punkt 4.1.1 under detta avtals giltighetstid görs tillgängliga för datamottagaren, ska tillägg 4 ändras i enlighet med detta på begäran av datahållaren.

Tills dess att tillägg 4 har ändrats och godkänts av parterna får datahållaren hålla inne eller tillfälligt avbryta delningen av de nya data som skyddas som företagshemligheter. I sådant fall ska datahållarens beslut vederbörligen motiveras och lämnas skriftligen till användaren utan oskäligt dröjsmål. Datahållaren ska också underrätta den behöriga myndighet som utsetts enligt artikel 37 i dataförordningen om att den har hållit inne eller avbrutit datadelningen och ange vilka åtgärder som inte har överenskommits eller genomförts.

4.1.4. De skyldigheter som anges i klausulerna 4.2 och 4.3 förblir i kraft efter avtalets upphörande, om inte parterna kommer överens om något annat.

4.2. **Skyddsåtgärder som vidtas av datamottagaren**

4.2.1. Datamottagaren måste tillämpa de skyddsåtgärder som anges i **tillägg 4** (nedan kallade *datamottagarens skyddsåtgärder*).

Parterna bör i ett separat tillägg ange alla detaljer om dessa åtgärder, inklusive för situationer när datamottagaren delar data med tredje part. Åtgärderna kan vara både tekniska (t.ex. kryptering, brandväggar, delad lagring osv.) och organisatoriska (t.ex. intern styrning, lämplig identitetshantering och åtkomstkontroller, involvering av en betrodd tredje part).

Eftersom åtgärderna måste vara proportionerliga kommer deras innehåll att variera beroende på vilken typ av företagshemligheter det rör sig om. Åtgärderna kommer också att bero på om i) åtkomst ska ges till den plats där data lagras eller ii) data ska överföras i sin helhet till datamottagaren. I det första fallet har datahållaren en högre grad av kontroll och kan själv tillämpa en del av skyddsåtgärderna, medan datamottagaren kan ha en lägre användningsnivå för dessa data. I vilket fall som helst måste båda parter fokusera på att uppnå dataförordningens avsedda verkningar. Därför måste de olika intressena balanseras utan att de avsedda verkningarna undergrävs.

4.2.2. Om datamottagaren enligt detta avtal och enligt det avtal som datamottagaren har ingått med användaren har rätt att göra data tillgängliga för en tredje part, kan datamottagaren dela data som skyddas som företagshemligheter om

(a) datamottagaren utan oskäligt dröjsmål informerar datahållaren om att data som skyddas som företagshemligheter kommer att göras tillgängliga för en tredje part, anger vilka data det rör sig om och lämnar datahållaren uppgifter om den tredje partens identitet, etableringsort och kontaktuppgifter,

(b) den tredje parten tillämpar de skyddsåtgärder som anges i tillägg 4.

4.2.3. [ALTERNATIV] [För att kontrollera om och i vilken utsträckning datamottagaren har genomfört och upprätthåller datamottagarens skyddsåtgärder, samtycker datamottagaren till att antingen i) årligen erhålla en rapport om säkerhetsöverensstämmelse från en oberoende tredje part som valts av datamottagaren, eller ii) årligen tillåta en revision av säkerhetsöverensstämmelse från en oberoende tredje part som valts av datahållaren – under förutsättning att denna oberoende tredje part har undertecknat ett sekretessavtal som tillhandahålls av datamottagaren. Sådana säkerhetsrevisionsrapporter måste visa att datamottagaren uppfyller klausul 4 och tillägg 4 som gäller vid den tidpunkten. Resultaten av revisionsrapporterna ska utan oskäligt dröjsmål lämnas till båda parterna.

Datamottagaren kan välja mellan i) och ii). Om en part anser att säkerhetsrevisionsrapporten är felaktig, behåller den rätten att erhålla en säkerhetsrevisionsrapport från en annan oberoende tredje part. Om denna rätt utövas, kommer båda oberoende tredjepartsrevisorerna tillsammans med parterna att diskutera eventuella skillnader mellan de två rapporterna och sträva efter att lösa eventuella olösta frågor i god tro.

Kostnaderna för sådana revisionsrapporter ska bäras enligt följande: (*ange villkoren för betalning av dessa kostnader*).

Denna klausul är markerad som ett alternativ, eftersom parterna kan komma överens om andra åtgärder för att kontrollera att användaren fullgör sina skyldigheter att genomföra och upprätthålla datamottagarens skyddsåtgärder.

4.3. **Skyddsåtgärder som vidtas av innehavaren av företagshemligheter**

4.3.1. Datahållaren får tillämpa de åtgärder som överenskommits i **tillägg 4** för att bevara konfidentialiteten för de data som skyddas som företagshemligheter (nedan kallade *skyddsåtgärder som vidtagits av innehavaren av företagshemligheter*).

4.3.2. Datahållaren får också ensidigt vidta lämpliga tekniska och organisatoriska skyddsåtgärder, såsom uppdatering av programvara, om dessa inte påverkar datamottagaren negativt enligt detta avtal.

4.3.3. Datamottagaren förbinder sig att inte ändra eller ta bort skyddsåtgärderna som vidtagits av innehavaren av företagshemligheter eller de åtgärder som vidtagits i enlighet med klausul 4.3.2, om inte parterna kommit överens om annat.

4.4. **Skyldighet att dela och rätt att vägra, hålla inne eller säga upp**

4.4.1. Om skyddsåtgärderna som vidtagits av datahållaren och innehavaren av företagshemligheter inte är tillräckliga för att på ett adekvat sätt skydda en viss uppgift som skyddas som företagshemlighet, kan datahållaren, genom att meddela datamottagaren med en detaljerad beskrivning av åtgärdernas otillräcklighet, begära att ytterligare nödvändiga tekniska eller organisatoriska åtgärder ska överenskommas. Om det efter en rimlig tidsperiod inte finns någon överenskommelse om sådana åtgärder och om behovet av sådana åtgärder är vederbörligen motiverat, t.ex. i en säkerhetsrevisionsrapport, kan datahållaren hålla inne eller avbryta delningen av de specifika data som avses. I sådant fall måste datahållaren meddela datamottagaren och den behöriga myndighet som utsetts enligt artikel 37 i dataförordningen. Meddelandet måste vara vederbörligen motiverat, ange vilka åtgärder som inte har överenskommits, i förekommande fall vilka företagshemligheter som berörs, och lämnas skriftligen utan oskäligt dröjsmål. Datahållaren måste fortsätta att dela alla data som skyddas som företagshemligheter utom dessa specifika data.

4.4.2. Om datahållaren under exceptionella omständigheter kan visa att det är mycket sannolikt att denne kommer att lida allvarlig ekonomisk skada av att vissa data som skyddas som företagshemlighet lämnas ut till datamottagaren trots att datamottagarens skyddsåtgärder och, i förekommande fall, skyddsåtgärderna som vidtagits av innehavaren av företagshemligheter har genomförts, får datahållaren avbryta delningen av de specifika data som avses.

Detta får endast ske efter vederbörligen motiverat meddelande till datamottagaren och den behöriga myndighet som utsetts enligt artikel 37 i dataförordningen.

Datahållaren måste dock fortsätta att dela alla data som skyddas som företagshemligheter utom dessa specifika data.

Vägran eller avbrytande av datadelning enligt artikel 5 i dataförordningen är endast tillåtet under exceptionella omständigheter. Meddelandet måste därför vara vederbörligen motiverat. Aspekter som kan beaktas är till exempel bristen på verkställbarhet av skyddet av företagshemligheter i länder utanför EU, arten och graden av konfidentialitet för den aktuella företagshemligheten eller den relevanta uppkopplade produktens unika och nya karaktär.

4.4.3. Om datamottagaren underlåter att genomföra och upprätthålla sina skyddsåtgärder, och om denna underlåtenhet är vederbörligen motiverad av datahållaren, t.ex. i en säkerhetsrevisionsrapport, har datahållaren rätt att hålla inne eller avbryta delningen av de specifika identifierade företagshemligheterna tills datamottagaren har löst incidenten.

I detta fall måste datahållaren utan oskäligt dröjsmål skriftligen lämna ett vederbörligen motiverat meddelande till datamottagaren och till den behöriga myndighet som utsetts enligt artikel 37 i dataförordningen.

4.4.4. Klausul 4.4.1 ger inte datahållaren rätt att säga upp avtalet. Klausulerna 4.4.2 eller 4.4.3 ger datahållaren rätt att säga upp avtalet endast med avseende på de specifika identifierade företagshemligheterna, och om

(a) samtliga villkor i klausul 4.4.2 eller klausul 4.4.3 har uppfyllts,

(b) parterna inte har nått någon lösning efter en rimlig tidsperiod, trots försök att nå en vänskaplig lösning, inklusive efter ingripande av den behöriga myndighet som utsetts enligt artikel 37 i dataförordningen, och

(c) datamottagaren inte har fått ett domstolsbeslut av en behörig domstol som förpliktar datahållaren att göra data tillgängliga och det inte finns något pågående domstolsförfarande för ett sådant beslut.

4.5. **Lagring av data som skyddas som identifierade företagshemligheter**

4.5.1. Om datahållaren utövar sin rätt att hålla inne eller avbryta delningen av data i enlighet med klausulerna 4.4.1, 4.4.2 och 4.4.3, måste denne se till att de data som frågan gäller lagras så att de kan göras tillgängliga för datamottagaren

(a) när lämpliga skyddsåtgärder har överenskommits och vidtagits, eller

(b) när en behörig myndighet eller domstol har fattat ett bindande beslut som kräver att datahållaren tillhandahåller dessa data till datamottagaren.

Denna skyldighet att lagra data upphör när en behörig myndighet eller domstol i ett bindande beslut tillåter radering av dessa lagrade data eller när avtalet upphör att gälla i enlighet med klausul 4.4.4.

4.5.2. Datahållaren ska stå för de kostnader som är nödvändiga för att lagra data enligt punkt 4.5.1. Datamottagaren ska dock täcka sådana kostnader i den utsträckning som innehållandet eller avbrytandet av datadelning sker i enlighet med punkt 4.4.3.

5. **Användning av data och delning med tredje part**

5.1. **Tillåten användning av datamottagaren**

Datamottagaren förbinder sig att behandla de data som ställs till förfogande enligt avtalet endast för de ändamål och på de villkor som överenskommits med den begärande användaren.

Datamottagaren måste radera dessa data när de inte längre är nödvändiga för det överenskomna ändamålet, såvida inte annat har överenskommits med den begärande användaren när det gäller data som inte är personuppgifter.

5.2. **Delning av data med tredje part**

5.2.1. Datamottagaren får inte göra data tillgängliga för en annan tredje part, såvida inte detta har överenskommits i avtalet med den begärande användaren, är förenligt med eventuella skyddsåtgärder som överenskommits med datahållaren och är förenligt med tillämplig unionsrätt eller nationell rätt.

Datamottagaren får under inga omständigheter göra de data som denne erhåller tillgängliga för ett företag som utsetts till grindvakt enligt artikel 3 i förordning (EU) 2022/1925 (lagen om digitala marknader).

5.2.2. Om datamottagaren får göra data tillgängliga för en tredje part måste datamottagaren vidta lämpliga avtalsmässiga, tekniska och organisatoriska åtgärder för att säkerställa att

(a) *(om tillämpligt)* den tredje parten tillämpar minst samma skyddsåtgärder som datamottagaren måste tillämpa enligt klausul 4.2 och respekterar de skyddsåtgärder som datahållaren vidtagit enligt klausul 4.3,

(b) den tredje parten använder data uteslutande på ett sätt som är förenligt med klausulerna 5.1 och 5.3,

(c) datahållaren har minst samma rättsmedel mot den tredje parten som mot datamottagaren för användning eller utlämnande av data som är förbjudet enligt klausul 5.3.

5.2.3. Utan hinder av klausulerna 5.2.1 och 5.2.2 får datamottagaren använda behandlingstjänster, t.ex. molntjänster (inklusive infrastruktur som en tjänst, plattform som en tjänst och programvara som en tjänst), värdtjänster eller liknande tjänster för att för egen räkning och på eget ansvar uppnå de överenskomna syftena enligt klausul 5.1. Tredje parter får också använda sådana tjänster för att för egen räkning och på eget ansvar uppnå de syften för vilka data delas med dem.

5.3. **Obehörig användning eller delning av data**

5.3.1. Datamottagaren får inte

(a) (i syfte att erhålla data) lämna falsk information till datahållaren, använda bedrägliga metoder eller tvångsmedel eller utnyttja luckor i datahållarens tekniska infrastruktur som är utformad att skydda dessa data, eller

(b) underlåta att upprätthålla de avtalsenliga tekniska eller organisatoriska åtgärder som överenskommits enligt klausulerna 4.2 och 4.3, eller

(c) utan datahållarens samtycke ändra eller ta bort tekniska skyddsåtgärder som datahållaren tillämpar för att förhindra obehörig åtkomst till data och för att säkerställa efterlevnaden av detta avtal, eller

(d) använda de data datamottagaren erhållit för obehöriga ändamål, i strid med klausul 5.1, eller

(e) använda data för att utveckla en produkt som konkurrerar med produkten, eller dela data med tredje part för detta ändamål, eller

(f) använda data för att få insikt om datahållarens ekonomiska situation, tillgångar och produktionsmetoder, eller dess användning av data, eller

(g) använda data på ett sätt som negativt påverkar säkerheten för produkten eller någon tillhörande tjänst, eller

(h) använda data för profilering av fysiska personer, såvida detta inte är nödvändigt för att tillhandahålla den tjänst som begärs av den begärande användaren, eller

(i) olagligt eller i strid med klausulerna 5.2.1 och 5.2.2 lämna ut data för en annan tredje part.

Om datamottagaren gör något av detta utgör det en grundläggande underlåtenhet att fullgöra sina skyldigheter enligt klausul 8.1.1 och medför de ytterligare konsekvenser som beskrivs i klausul 5.3.2.

5.3.2. I de fall som avses i klausul 5.3.1 måste datamottagaren utan oskäligt dröjsmål följa datahållarens eller den begärande användarens begäran om att

(a) informera den begärande användaren om obehörig användning eller utlämnande av data och åtgärder som vidtagits för att sätta stopp för detta,

(b) radera de data som datahållaren har gjort tillgängliga enligt detta avtal, eller som har erhållits på ett obehörigt eller otillbörligt sätt, samt alla kopior av dessa,

(c) ersätta datahållaren, den begärande användaren eller annan skyddad tredje part för skada som lidits till följd av den obehöriga användningen eller utlämnandet, och

(d) upphöra med tillverkning, erbjudande, utsläppande på marknaden eller användning av varor, härledda data eller tjänster som framställts på grundval av kunskap som erhållits genom dessa data, eller import, export eller lagring av varor som innebär intrång för dessa ändamål, och

(e) förstöra alla varor som innebär intrång, om i) det finns en allvarlig risk för att den olagliga användningen av data kommer att orsaka betydande skada för datahållaren, innehavaren av företagshemligheter eller användaren, eller ii) om denna åtgärd inte skulle vara oproportionerlig med hänsyn till intressena för datahållaren, innehavaren av företagshemligheter eller användaren.

6. **Ersättning för tillhandahållande av åtkomst till data**

Parterna bör i själva avtalet eller i ett separat tillägg fastställa detaljerna för ersättningen.

De bör åtminstone komma överens om följande:

— Ersättningsbeloppet och valutan.

— Tidpunkten för betalningen.

— Betalningsvillkoren.

I enlighet med dataförordningen kan sådan ersättning alltid omfatta ersättning för de kostnader som uppkommit för att göra data tillgängliga. Den kan också omfatta en marginal, utom när datamottagaren är ett litet eller medelstort företag eller en ideell organisation. Ersättningen måste i alla fall vara rimlig.

I enlighet med artikel 9.2 i dataförordningen ska ”[k]ostnader för att göra data tillgängliga, inbegripet särskilt de kostnader som är nödvändiga för formatering av data, spridning med elektroniska medel och lagring” samt, om ersättningen inkluderar en marginal, ”[i]nvesteringar i insamling och framställning av data, i förekommande fall med beaktande av huruvida andra parter har bidragit till att inhämta, generera eller samla in datan i fråga” beaktas vid fastställandet av ersättningen.

Enligt artikel 9.3 i dataförordningen kan ersättningen också bero på datas volym, format och karaktär. Enligt artikel 9.7 i dataförordningen måste datahållaren i alla händelser tillhandahålla information som i tillräcklig detalj beskriver grunden för beräkningen av ersättningen, så att datamottagaren kan bedöma om de lagstadgade kraven är uppfyllda.

6.1. **(Tillämpligt om datamottagaren uppfyller kraven för att klassificeras som ett litet eller medelstort företag/en ideell forskningsorganisation)**

6.1.1. Datamottagaren försäkrar att denne är ett litet eller medelstort företag enligt definitionen i rekommendation 2003/361/EG *eller* en ideell forskningsorganisation. Datamottagaren förklarar vidare att denne inte har några partnerföretag eller anknutna företag (*företag*) enligt definitionen i artikel 3 i bilagan till rekommendation 2003/361/EG som inte uppfyller kraven för att klassificeras som ett litet eller medelstort företag.

[ALTERNATIV] [Bevis för ovanstående finns i **tillägg 3**.]

6.1.2. Parterna är överens om att datamottagaren ska betala ersättning till datahållaren [ALTERNATIV 1] [enligt följande: (*ange*)] [ALTERNATIV 2] [enligt **tillägg 3**].

6.1.3. Datahållaren försäkrar att den överenskomna ersättningen inte överstiger de kostnader som är direkt relaterade till att göra data tillgängliga för datamottagaren och som är hänförliga till begäran. Dessa kostnader inkluderar de kostnader som är nödvändiga för återgivning av data, spridning på elektronisk väg och lagring av data, men inte för datainsamling eller dataproduktion.

Information om grunden för beräkningen av ersättningen, som gör det möjligt för datamottagaren att kontrollera att dessa krav är uppfyllda, tillhandahålls av datahållaren i **tillägg 3**.

6.1.4. Datamottagaren ska omedelbart informera datahållaren om alla förändringar som ifrågasätter deras klassificering som ett litet eller medelstort företag.

Om datamottagaren upphör att uppfylla kraven för att klassificeras som ett litet eller medelstort företag, åtar sig parterna att inleda förhandlingar om ett rimligt ersättningsbelopp. Om ingen överenskommelse nås inom en rimlig tidsperiod, kan datahållaren avbryta delningen av data genom att meddela datamottagaren.

I detta fall måste datahållaren se till att dessa data lagras, så att de kan göras tillgängliga för datamottagaren när ersättningen har fastställts eller när en behörig myndighet eller domstol har fattat ett bindande beslut som kräver att datahållaren tillhandahåller dessa data till datamottagaren.

Datahållaren ska stå för de kostnader som är nödvändiga för att lagra data. Datamottagaren måste dock ersätta datahållaren för eventuella ekonomiska skador som uppstått på grund av att datamottagaren underlåtit att informera datahållaren.

6.2. **(Tillämpligt om datamottagaren inte uppfyller kraven för att klassificeras som ett litet eller medelstort företag/en ideell forskningsorganisation)**

6.2.1. Parterna är överens om att datamottagaren ska betala ersättning till datahållaren [ALTERNATIV 1] [enligt följande: (*ange*)] [ALTERNATIV 2] [enligt **tillägg 3**].

Information om grunden för beräkningen av ersättningen, som gör det möjligt för datamottagaren att kontrollera att dessa krav är uppfyllda, tillhandahålls av datahållaren i **tillägg 3**.

6.2.2. (*tillämpligt vid ekonomisk ersättning*) Om betalningen av ersättningen försenas ska datamottagaren betala datahållaren ränta på försenad ersättning från den tidpunkt då betalningen förfaller till betalning till den tidpunkt då betalningen sker, i enlighet med tillämplig lag.

6.2.3. Om datamottagaren börjar uppfylla kraven för att klassificeras som ett litet eller medelstort företag och informerar datahållaren om detta, åtar sig parterna att ändra beloppet för den rimliga ersättningen i enlighet med artikel 9.4 i dataförordningen.

7. **Datum för tillämpning, avtalets löptid och uppsägning**

7.1. **Datum för tillämpning och löptid**

7.1.1. Detta avtal [ALTERNATIV 1] [träder i kraft omedelbart] [ALTERNATIV 2] [träder i kraft från och med den (*ange datum*)].

7.1.2. [ALTERNATIV] [Detta avtal ingås för [ALTERNATIV 1] [obestämd tid] [ALTERNATIV 2] [en fast period på (*ange*)], med förbehåll för eventuella skäl för upphörande eller uppsägning enligt detta avtal.]

Vid bedömningen av avtalets löptid bör parterna i första hand utgå från användarens begäran och det avtal som ingåtts mellan användaren och datamottagaren. Om begäran avser en **engångsleverans** av data är det tillräckligt att komma överens om tillämpningsdatumet.

Om begäran avser en **kontinuerlig leverans** av data måste parterna komma överens om avtalets löptid och välja antingen en obestämd tidsperiod eller en fast tidsperiod, beroende på om den begärande användaren har angett en viss tidsperiod.

7.1.3. [ALTERNATIV] [Datahållaren måste börja tillhandahålla data till datamottagaren [ALTERNATIV 1] [utan oskäligt dröjsmål efter det att avtalet trätt i kraft] [ALTERNATIV 2] [den (*ange datum och, i förekommande fall, ytterligare uppgifter om tidpunkten*)].]

Normalt vill parterna att fullgörandet ska påbörjas direkt efter det att avtalet har trätt i kraft. Detta är dock inte nödvändigtvis fallet, t.ex. om en eller båda parter fortfarande måste förbereda sig för att fullgörandet ska kunna påbörjas.

7.2. **Uppsägning**

7.2.1. Oavsett den avtalade avtalsperioden enligt klausul 7.1.1 och utan att det påverkar klausul 2.4.3 upphör detta avtal att gälla

(a) vid förstörelse av produkten eller permanent upphörande av den tillhörande tjänsten, eller när produkten eller den tillhörande tjänsten på ett oåterkalleligt sätt förlorar sin förmåga att generera data, eller

(b) när båda parter är överens om detta.

7.2.2. Datamottagaren kan säga upp avtalet när som helst under avtalsperioden genom att meddela datahållaren (*ange period*). Datamottagaren måste meddela den begärande användaren att avtalet har sagts upp.

[ALTERNATIV] Om datamottagaren säger upp avtalet enligt denna klausul före (*ange tidpunkt eller minsta avtalsperiod*), måste denne ersätta datahållaren för de kostnader som datahållaren har haft för att göra data tillgängliga, enligt följande: (*ange*).

Det kan förekomma fall där datahållaren har kostnader för att göra data tillgängliga för datamottagaren, till exempel genom att anpassa sin digitala infrastruktur, i förvissning om att dessa kostnader kommer att amorteras över tid.

I detta fall kan datahållaren vilja säkerställa att denne får ersättning från datamottagaren.

7.3. **Verkningar av upphörande och uppsägning**

7.3.1. När avtalsperioden löper ut eller detta avtal sägs upp befrias båda parter från sin skyldighet att utföra och ta emot framtida prestationer, men detta påverkar inte de rättigheter och skyldigheter som har uppkommit fram till tidpunkten för upphörandet eller uppsägningen.

Upphörande eller uppsägning påverkar inte bestämmelser som ska gälla även efter det att avtalet har upphört, i synnerhet begränsningar av datamottagarens tillåtna användning och delning av data enligt klausul 5, klausul 4 om företagshemligheter, klausul 9.1 om konfidentialitet, klausul 9.5 om tillämplig lag och klausul 9.7 om tvistlösning.

7.3.2. [ALTERNATIV 1] [Datahållaren måste vidta lämpliga åtgärder för att underlätta utträde, i enlighet med vad datamottagaren rimligen kan förvänta sig.] [ALTERNATIV 2] [Datahållaren måste vidta följande åtgärder för att underlätta utträde: (*ange*).]

Parterna kan överväga om datamottagaren behöver några åtgärder för att underlätta utträde.

Detta är till exempel relevant om datamottagaren hade tillåtelse att extrahera data från ett medium som kontrolleras av datahållaren men ännu inte hade extraherat data, eftersom datamottagaren inte förväntade sig att avtalet skulle sägas upp.

8. **Åtgärder vid avtalsbrott**

Parterna kan komma överens om att inte bara fastställa specifika rättigheter och skyldigheter avseende data (varav många redan följer av dataförordningen), utan även om allmänna avtalsrättsliga frågor, såsom en avtalsslutande parts rättigheter och åtgärder om den andra avtalsslutande parten inte fullgör sina skyldigheter.

För sådana allmänna avtalsrättsliga frågor kan parterna vilja förlita sig på lagstadgade standardregler eller andra avtalsmallar.

Om de vill använda dessa standardavtalsvillkor bör de se till att dessa är förenliga med eventuell tvingande nationell rätt som kan vara tillämplig på avtalet.

8.1. **Fall av underlåtenhet att fullgöra sina skyldigheter**

8.1.1. En parts underlåtenhet att fullgöra en skyldighet är av grundläggande betydelse om

(a) underlåtenheten väsentligen berövar den andra parten det som den hade rätt att förvänta sig enligt detta avtal, såvida inte den part som underlåtit att fullgöra sina skyldigheter inte kunde förutse och rimligen inte kunde ha förutsett detta resultat, eller

(b) det av omständigheterna framgår att man i framtiden inte kan förlita sig på den part som underlåtit att fullgöra sina skyldigheter.

8.1.2. En parts underlåtenhet är ursäktlig om den beror på ett hinder utanför dess kontroll och den parten rimligen inte kunde förväntas ta hänsyn till hindret vid tidpunkten för ingåendet av detta avtal, eller undvika eller övervinna hindret eller dess konsekvenser.

Om hindret endast är tillfälligt ska underlåtenheten vara ursäktad för den period som hindret består. Om förseningen dock innebär en grundläggande underlåtenhet att fullgöra sina skyldigheter, kan den andra parten behandla den som sådan.

Den part som underlåter att fullgöra sina skyldigheter måste se till att den andra parten utan oskäligt dröjsmål får kännedom om hindret och dess inverkan på partens förmåga att fullgöra sina skyldigheter, efter det att den part som underlåter att fullgöra sina skyldigheter har fått kännedom om eller rimligen kunde förväntas ha fått kännedom om dessa omständigheter. Den andra parten har rätt till skadestånd för ekonomisk skada som uppstår till följd av att ett sådant meddelande inte mottagits.

8.2. **Åtgärder vid underlåtenhet att fullgöra sina skyldigheter**

8.2.1. Om en part inte fullgör sina skyldigheter, ska den andra parten ha de rättsmedel som anges i följande klausuler, utan att det påverkar de rättsmedel som finns tillgängliga enligt tillämplig lag.

8.2.2. Rättsmedel som inte är sinsemellan oförenliga får kombineras.

8.2.3. En part får inte utnyttja ett rättsmedel i den mån det orsakar den andra partens underlåtenhet att fullgöra sina skyldigheter, till exempel om en brist i den egna datainfrastrukturen har gjort det omöjligt för den andra parten att fullgöra sina skyldigheter. En part får inte heller åberopa ett skadeståndsanspråk i den mån den kunde ha minskat skadan genom att vidta rimliga åtgärder.

8.2.4. Den skadelidande parten kan

(a) begära att den part som inte fullgör sina skyldigheter utan oskäligt dröjsmål fullgör sina skyldigheter enligt detta avtal, såvida detta inte är olagligt eller omöjligt eller om specifikt fullgörande skulle medföra kostnader för den part som inte fullgör sina skyldigheter som är oproportionerliga i förhållande till den fördel som den andra parten skulle erhålla,

(b) avstå från att fullgöra sina skyldigheter enligt detta avtal, såvida detta inte kan förväntas orsaka den part som inte fullgör sina skyldigheter en skada som är uppenbart oproportionerlig i förhållande till allvaret i underlåtenheten (om tillämpligt) [förutsatt att alla villkor i klausul 4.4.4 är uppfyllda, om datamottagaren underlåter att genomföra eller upprätthålla de skyddsåtgärder för datamottagaren som överenskommits i klausul 4.2.1],

(c) säga upp avtalet med omedelbar verkan utan påföljd genom att meddela den andra parten, om

i) den andra partens underlåtenhet är grundläggande, eller

ii) i fall av underlåtenhet som inte är grundläggande, den skadelidande parten har meddelat en rimlig tidsfrist för att avhjälpa underlåtenheten och tidsfristen har löpt ut utan att den andra parten har fullgjort sina skyldigheter,

iii) *(om tillämpligt)* [förutsatt att samtliga villkor som anges i klausul 4.4.5 är uppfyllda, i de fall som beskrivs i klausulerna 4.4.2 eller 4.4.3,]

(d) kräva skadestånd för ekonomisk skada som den andra parten har orsakat genom underlåtenhet att fullgöra sina skyldigheter och som inte är undantagen enligt klausul 8.1.2; den part som underlåter att fullgöra sina skyldigheter är endast ansvarig för skador som den förutsåg eller rimligen kunde ha förutsett vid tidpunkten för ingåendet av detta avtal som ett resultat av sin underlåtenhet att fullgöra sina skyldigheter, såvida inte underlåtenheten var uppsåtlig eller grovt vårdslös.

8.2.5. [ALTERNATIV] Om en part underlåter att fullgöra sina skyldigheter enligt detta avtal ska den i alla fall betala de straffavgifter som anges i detalj i **tillägg 5**, vilka parterna anser vara skadestånd i den mening som avses i klausul 8.2.4 d. Den part som underlåter att fullgöra sina skyldigheter har rätt att begära att straffavgiften sänks till ett rimligt belopp om den kan bevisa att straffavgiften är grovt överdriven i förhållande till den skada som uppstått till följd av underlåtenheten.

Parterna kanske vill fastställa påföljder för vissa typer av underlåtenhet, eftersom det kan vara alltför betungande för den skadelidande parten att bevisa storleken på den faktiska skada som orsakats av t.ex. underlåtenhet att tillhandahålla data. Påföljderna bör vara proportionerliga.

9. Allmänna bestämmelser

9.1. Konfidentialitet

9.1.1. Följande information ska betraktas som konfidentiell:

(a) Information som avser företagshemligheter, ekonomisk situation eller andra aspekter av en parts verksamhet, såvida inte den parten har offentliggjort denna information.

(b) Information som anger grunden för beräkningen av rimlig ersättning.

(c) Information som avser den begärande användaren och tredje part, såvida de inte redan har offentliggjort denna information.

9.1.2. Båda parterna samtycker till att vidta alla rimliga åtgärder för att lagra konfidentiell information på ett säkert sätt och att inte göra sådan information tillgänglig för tredje part, såvida inte

(a) en av parterna har en laglig skyldighet att göra relevant information tillgänglig, t.ex. för att fullgöra skyldigheten att tillhandahålla information som visar att det inte har förekommit någon diskriminering i enlighet med artikel 8.3 i dataförordningen, eller

(b) det är nödvändigt för en av parterna att göra relevant information tillgänglig för att fullgöra sina skyldigheter enligt detta avtal, eller

(c) en av parterna har erhållit förhandsgodkännande från den andra parten eller den part som tillhandahåller den konfidentiella informationen eller som påverkas av dess utlämnande.

9.1.3. I alla händelser får datahållaren lämna ut eller tillhandahålla [ALTERNATIV 1] [avtalet till den begärande användaren] [ALTERNATIV 2] [sådan information till den begärande användaren som är nödvändig för att datahållaren ska kunna visa att denne fullgör sina skyldigheter i) gentemot datamottagaren enligt artikel 5 i dataförordningen eller ii) som följer av ett avtal som ingåtts med den begärande användaren enligt artikel 4.6 i dataförordningen].

9.1.4. Dessa skyldigheter avseende konfidentialitet gäller även efter avtalets upphörande under en period av (*ange period*).

9.1.5. Dessa skyldigheter avseende konfidentialitet upphäver inte strängare förpliktelser enligt i) den allmänna dataskyddsförordningen, ii) bestämmelserna om genomförande av direktiv 2002/58/EG eller direktiv (EU) 2016/943, eller iii) annan unionsrätt eller nationell rätt.

9.2. **Icke-diskriminering**

Datahållaren försäkrar att villkoren i detta avtal och alla rutiner som rör dess fullgörande inte diskriminerar mellan jämförbara kategorier av datamottagare, inklusive deras partner eller anknutna företag, enligt definitionen i artikel 3 i bilagan till rekommendation 2003/361/EG, när data görs tillgängliga.

Om datamottagaren anser att de villkor under vilka data har gjorts tillgängliga för denne är diskriminerande, ska datahållaren på begäran av datamottagaren utan oskäligt dröjsmål tillhandahålla information som visar att ingen diskriminering har förekommit.

9.3. **Kommunikationsmedel**

Alla meddelanden eller annan kommunikation som krävs enligt detta avtal måste vara skriftliga och kan levereras personligen, skickas med förbetald post eller överföras elektroniskt, inklusive e-post, förutsatt att avsändaren behåller bevis på att de har skickats till nedanstående adresser:

Part	Kontaktperson	E-post	Telefon	Adress
Användare	[Namn]/[Befattning]	[E-post]	[Telefon]	[Adress]
Datamottagare	[Namn]/[Befattning]	[E-post]	[Telefon]	[Adress]

Sådana meddelanden eller kommunikationer ska anses ha mottagits

(a) om de levereras personligen, på leveransdagen,

(b) om de skickas med förbetald post, den tredje arbetsdagen efter att de postats,

(c) om de skickas elektroniskt, på överföringsdagen, förutsatt att avsändaren inte har mottagit något felmeddelande som indikerar att leveransen misslyckats.

9.4. **Hela avtalet, ändringar och avskiljbarhet**

9.4.1. Detta avtal (tillsammans med dess **tillägg** som hänvisas till i avtalet) utgör hela avtalet mellan parterna avseende avtalets innehåll och ersätter med avseende på innehållet alla tidigare muntliga eller skriftliga avtal och uppgörelser mellan parterna avseende avtalets innehåll.

9.4.2. Alla ändringar av detta avtal är endast giltiga om de har godkänts skriftligen av parterna, inklusive i elektronisk form.

9.4.3. Om någon bestämmelse i detta avtal av någon anledning befinns vara ogiltig, upphävbar eller icke verkställbar, och om denna bestämmelse kan särskiljas från övriga villkor i avtalet, ska de övriga bestämmelserna fortsätta att vara giltiga och verkställbara. Eventuella luckor eller oklarheter i detta avtal ska hanteras i enlighet med klausul 9.6.

9.5. **Tillämplig lag**

Detta avtal måste regleras av lagen i (*ange medlemsstat*).

9.6. **Tolkning**

9.6.1. Detta avtal ingås av parterna mot bakgrund av parternas rättigheter och skyldigheter enligt dataförordningen. Alla bestämmelser i detta avtal ska tolkas så att de överensstämmer med dataförordningen och annan unionsrätt eller nationell lagstiftning som antagits i enlighet med unionsrätten, samt all tillämplig nationell rätt som är förenlig med unionsrätten och som inte kan frångås genom avtal.

9.6.2. Om någon lucka eller oklarhet i detta avtal inte kan lösas på det sätt som anges i klausul 9.6.1, ska detta avtal tolkas mot bakgrund av de tolkningsregler som föreskrivs i tillämplig lag (se klausul 9.5).

9.7. **Tvistlösning**

9.7.1. Parterna är överens om att göra sitt yttersta för att lösa tvister i godo och, innan de väcker talan vid domstol, att hänskjuta tvisten till (*ange namn och kontaktuppgifter för ett särskilt tvistlösningsorgan eller, för tvister som faller inom dess behörighet, hänvisa till ett tvistlösningsorgan i en medlemsstat som uppfyller villkoren i artikel 10 i dataförordningen*).

[ALTERNATIV] [Domstolarna i (*ange medlemsstat*) har exklusiv behörighet att pröva mål som rör detta avtal.]

Tillägg 1

(bevis på begäran och, i förekommande fall, eventuell fullmakt)

[ska utarbetas av parterna]

Tillägg 2

(uppgifter om de data som omfattas av avtalet och om villkoren för åtkomst)

I detta tillägg ska parterna ange detaljer om de data som omfattas av avtalet, om villkoren för åtkomst och om de medel och den information som krävs för att få åtkomst till och använda data, enligt överenskommelsen i punkterna 3.1 och 3.2.

Detta tillägg innehåller endast en förteckning över de viktigaste punkterna som parterna bör komma överens om. Både formen och innehållet ska anpassas av parterna så att det motsvarar deras behov. Parterna kan lägga till ytterligare punkter i denna förteckning.

A. **Specificering av datas innehåll**

I tillägget ska de produktdata och data från tillhörande tjänster som omfattas av avtalet sorteras och listas, med angivande av innehållet i dessa data och insamlingsfrekvensen (strukturerad förteckning över datapunkter eller exakta datakategorier).

B. **Lagringstid**

I tillägget ska lagringstiden anges, så att användaren informeras om hur länge data är tillgängliga. Detta kan göras på ett detaljerat sätt för varje datapunkt eller grupp av datapunkter.

C. **Dataordning**

I tillägget ska anges om alla eller delar av data är särskilda data som regleras av en särskild ordning. I tillägget kan t.ex. anges huruvida och vilka data som kan betraktas som personuppgifter.

D. **Datastruktur och dataformat**

I tillägget ska anges i vilket strukturerat, allmänt använt och maskinläsbart format data görs tillgängliga.

E. **Överförings-/åtkomstmedium**

I tillägget ska anges vilket säkert och bekvämt elektroniskt medium som datahållaren kan använda för att göra data tillgängliga för användaren, antingen genom överföring eller åtkomst.

F. **Tidpunkt för åtkomst till data**

I tillägget ska hastigheten, frekvensen och andra tidsrelaterade parametrar för åtkomst till data anges, till exempel i realtid, nära realtid, kontinuerligt, utan oskäligt dröjsmål, med en viss frekvens.

G. **Startdatum**

I tillägget ska startdatumet anges då datahållaren kommer att göra data tillgängliga för datamottagaren.

H. **Information som är nödvändig för att datamottagaren ska kunna utöva sina åtkomsträttigheter**

I tillägget kan den information anges som är nödvändig för att datamottagaren ska kunna utöva sina åtkomsträttigheter. Informationen kan omfatta en kontaktperson som kan lösa tekniska problem, både hos datahållaren och hos datamottagaren.

Tillägg 3

(bevis på datamottagarens storlek och detaljer om beräkningen av ersättningen)

[ska utarbetas av parterna]

Tillägg 4

(företagshemligheter)

[ska utarbetas av parterna]

BILAGA V

STANDARDAVTALSVILLKOR

för avtal om frivillig delning av data mellan datadelare och datamottagare

Dessa standardavtalsvillkor är avsedda för avtal där datadelningen är frivillig mellan en datadelare och en datamottagare, dvs. datadelaren är inte skyldig att dela data enligt förordning (EU) 2023/2854 (nedan kallad *dataförordningen*) eller enligt någon annan rättslig skyldighet i unionsrätten (t.ex. artiklarna 6.9 och 6.10 i lagen om digitala marknader) eller nationell rätt.

Den viktigaste nyheten i dataförordningen för sådana förhållanden är att den i artikel 13 innehåller en prövning av oskäliga avtalsvillkor. Avtalsvillkor som rör åtkomst till och användning av data, eller ansvar och rättsmedel vid överträdelse eller upphörande av datarelaterade skyldigheter, som ensidigt har ålagts ett företag av ett annat företag, är inte bindande om de är oskäliga.

Även om detta avtal inte är avsett att ersätta befintliga avtal om frivillig datadelning, kan det användas som riktmärke för att bedöma skäligheten i klausuler i befintliga avtal.

I fall av obligatorisk delning av produktdata och relaterade tjänstedata enligt dataförordningen ska antingen ”Standardavtalsvillkor för avtal mellan datahållare och datamottagare om tillhandahållande av data på begäran av användare av uppkopplade produkter och tillhörande tjänster” (artikel 5 i dataförordningen) eller ”Standardavtalsvillkor för avtal om åtkomst till och användning av data mellan datahållare och användare av uppkopplade produkter och tillhörande tjänster” (artikel 4 i dataförordningen) användas.

Andra obligatoriska fall av datadelning ska hanteras separat av parterna, som ska se till att både skyldigheterna enligt den specifika lagbestämmelsen och skyldigheterna enligt kapitel III i dataförordningen uppfylls. Särskilda villkor som utarbetats av Europeiska kommissionen eller en medlemsstat kan tillämpas på ett obligatoriskt fall av datadelning av detta slag.

1. **Avtalsparter**

Detta avtal om åtkomst till och användning av data ingås mellan

(*ange namn, kontaktuppgifter och ytterligare referenser*) (*datadelaren*)

och

(*ange namn, kontaktuppgifter och ytterligare referenser*) (*datamottagaren*)

i detta avtal gemensamt benämnda *parterna* och var för sig *parten*.

En datadelare kan vara ett företag som

— innehar data, och

— har rätt att frivilligt göra data tillgängliga, och

— kontrollerar, beroende på fallet, egenskaperna hos data eller sättet att få åtkomst till data, på ett sådant sätt att de kan uppfylla skyldigheterna i dessa standardavtalsvillkor (om så inte är fallet kan ett annat avtal vara mer lämpligt).

Observera att för delning av personuppgifter krävs efterlevnad av tillämplig dataskyddslagstiftning (inklusive krav på rättslig grund och, när data delas med en datamottagare i ett tredjeland, efterlevnad av kraven för internationell dataöverföring).

För användningsfall som rör dataförordningen kan datadelaren till exempel vara

— en datahållare enligt artikel 2.13 i förordning (EU) 2023/2854 som har rätt att dela produktdata och data från tillhörande tjänster eller som vill dela härledda eller avledda data,

— en användare av en uppkopplad produkt eller tillhörande tjänst till vilken data har överförts av en datahållare (inklusive till exempel data från en virtuell assistent som interagerar med produkten eller den tillhörande tjänsten),
— en tidigare datamottagare enligt artikel 2.14 i förordning (EU) 2023/2854 som nu har rätt att använda och göra data tillgängliga i enlighet med sina avtal med användaren och datahållaren.

För andra användningsfall kan datadelaren till exempel vara

— en jordbrukare som vill dela markdata för att förbättra sina växtmönster med sin AI-leverantör eller för att träna, förbättra eller utveckla nya AI-system med en annan AI-leverantör,

— ett företag som vill sälja delar av sina affärsdata till ett annat företag,

— ett universitet som vill sälja data till ett sociologiskt forskningsinstitut för att skapa statistik,

— ett it-företag som vill delta i ett datanätverk för cybersäkerhetsincidenter för att främja hanteringen av incidenter.

En datamottagare kan vara ett företag som datadelaren gör data tillgängliga för och som tar emot och använder data för sina egna affärsändamål inom ramen för detta avtal som motpart till datadelaren.

Definitionen av datamottagare i detta avtal omfattar alla mottagande parter av alla typer av datadelning, inte bara datamottagare inom de obligatoriska situationer för datadelning som anges i dataförordningen.

2. **Data som omfattas av avtalet**

De data som omfattas av detta avtal består av de data som anges i **tillägg 1** (*data*). Om alla eller delar av de data som tillhandahålls enligt detta avtal omfattas av en särskild ordning (med undantag för personuppgifter som särskilt behandlas i klausul 3.2), förbinder sig datadelaren att identifiera sådana data i **tillägg 2** samt att vidta lämpliga åtgärder för att skydda sådana data i enlighet med den tillämpliga ordningen.

Identifiering av särskild ordning

Eftersom dessa villkor avser rent frivillig datadelning har datadelaren ingen skyldighet att dela data som omfattas av en särskild rättsordning (i synnerhet och i motsats till obligatorisk datadelning enligt dataförordningen finns det ingen skyldighet att dela data som skyddas som företagshemligheter). Om data som omfattas av den särskilda ordningen inte delas behöver de inte anges i tillägg 2. Om de däremot delas måste de anges och skyddas i enlighet därmed.

Data som identifieras som sådana i tillägg 2 kan till exempel

— skyddas som företagshemligheter av datadelaren, i vilket fall de omfattas av klausulen om ”företagshemligheter”,

— betraktas som konfidentiella av datadelaren, i vilket fall de skyddas enligt klausulen om ”konfidentialitet”,

— skyddas av rätten av sitt eget slag (sui generis) avseende databaser eller andra immateriella rättigheter, i vilket fall klausulen om ”immateriella rättigheter” kommer att tillämpas,

— omfattas av en sektorsspecifik förordning (t.ex. energi, försvar, säkerhet, finans, kliniska prövningar osv.), inklusive förordningar som rör gemensamma europeiska dataområden,

— påverkas av konkurrensrättsliga begränsningar, eller

— skyddas av någon annan relevant rättsordning som parterna vill framhålla.

Beskrivningen av de data som omfattas av den relevanta rättsordningen bör kompletteras med information som är nödvändig för att datamottagaren ska kunna använda data på ett lagligt och säkert sätt (t.ex. när det gäller skydd av immateriella rättigheter, licensinformation och tredje parts upphovsrätt).

Det särskilda fallet med gemensamma europeiska dataområden

I vissa situationer kan data delas inom ramen för ett domänspecifikt gemensamt europeiskt dataområde. Denna datadelning bör genomföras i enlighet med bestämmelserna i den relevanta förordningen som är tillämplig på ett sådant dataområde, när det gäller obligatorisk datadelning enligt en sådan förordning. Utanför ramen för obligatorisk datadelning enligt den relevanta förordningen som är tillämplig på ett dataområde är frivillig datadelning fortfarande möjlig. I detta fall kan denna uppsättning villkor användas.

3. **Grunden för avtalet**

3.1. **Ursprunget till data**

3.1.1. Datadelaren försäkrar härmed att data som tillhandahålls enligt detta avtal härrör från följande källor: *(ange alla datakällor och, om möjligt, data som tillhandahålls av varje källa)*

Parterna kan ange olika typer av källor, till exempel

— produktdata eller data från tillhörande tjänster enligt dataförordningen,

— andra data som härrör från en produkt eller tillhörande tjänst som inte uppfyller kraven för produktdata eller data från tillhörande tjänster enligt dataförordningen (t.ex. härledda data eller data som härrör från annan programvara, såsom demografiska data som användaren har angett i en app),

— data som härrör från externa källor, till exempel data som tillhandahålls datadelaren av en tredje part i relation till sådan tredje parts produkter eller användare,

— data som skapats av datadelaren (självständigt), till exempel kundregister som skapats av datadelarens anställda i dess system för kundrelationshantering, tabeller, bearbetade data, härledda data, sammanslagna data osv.

Garantier är i allmänhet en följd av att datadelaren tillhandahåller data och att datamottagaren inte kan verifiera lagligheten av sådana data och deras ursprung. I sådana fall måste datamottagaren förlita sig på datadelaren och vill kanske erhålla vissa garantier i detta avseende. Garantier kan dock vara irrelevanta i situationer där datamottagaren är bättre lämpad att kontrollera och/eller ta risken avseende data – till exempel på grund av att datadelaren är ett litet eller medelstort företag och/eller att data hämtas direkt från produkten.

3.1.2. Datadelaren försäkrar att

(a) *(om tillämpligt)* eftersom data innehåller icke-personliga produktdata eller data från tillhörande tjänster (enligt definitionen i förordning (EU) 2023/2854 om harmoniserade regler för skälig åtkomst till och användning av data (*dataförordningen*)) och datadelaren enligt detta avtal har åtkomst till data i egenskap av datahållare, är behandlingen och delningen av sådana data, i enlighet med artikel 4.13 i dataförordningen, föremål för ett avtal med respektive användare enligt definitionen i artikel 2.12 i dataförordningen (*användare*), och att detta avtal tillåter att data delas för de ändamål som beaktas i detta avtal,

(b) *(om tillämpligt)* eftersom data innehåller produktdata eller data från tillhörande tjänster och datadelaren enligt detta avtal har fått åtkomst till dessa i egenskap av datamottagare enligt artikel 5 i dataförordningen, bryter detta avtal inte mot avtalsenliga åtaganden med användaren och datahållaren och skyldigheter enligt dataförordningen,

(c) den äger eller innehar tillräckliga juridiska och/eller avtalsenliga rättigheter till data utan att kränka eller göra intrång i andras rättigheter, och det inte finns några pågående åtgärder, stämningar eller förfaranden mot datadelaren som, om de avgörs till datadelarens nackdel, skulle ha en väsentlig negativ inverkan på dess förmåga att bevilja de rättigheter som beviljas enligt detta avtal,

(d) om inte annat anges i **tillägg 2** och utan att det påverkar klausul 3.2, har datadelaren på egen bekostnad erhållit och kommer att upprätthålla under avtalets giltighetstid och för avtalets syfte alla tillstånd, licenser och fullmakter som krävdes för att datamottagaren skulle kunna dela och använda data som erhållits från eller tillhandahållits av en tredje part.

3.1.3. *(om tillämpligt)* Eftersom data innehåller produktdata eller data från tillhörande tjänster (enligt definitionen i dataförordningen) och datadelaren enligt detta avtal har fått åtkomst till dessa i enlighet med artikel 4 i dataförordningen i egenskap av användare, försäkrar datamottagaren att denne inte är utsedd till grindvakt enligt artikel 3 i förordning (EU) 2022/1925 (*lagen om digitala marknader*).

3.1.4. [ALTERNATIV] [Varje part ska säkerställa att alla data, filer eller programvara som överförs till den andra parten enligt detta avtal är fria från virus, skadeprogram, utpressningsprogram eller annan skadlig kod som kan äventyra integriteten, säkerheten eller funktionaliteten hos den andra partens system.

3.1.5. [ALTERNATIV] [Varje part ska säkerställa att alla data, filer eller programvara som överförs till den andra parten enligt detta avtal härrör från datainsamling som uppfyller tillämpliga standarder (*ange: yrkesmässiga standarder, etiska branschstandarder, cybersäkerhetsstandarder, forskningsstandarder och/eller AI-standarder*).]

3.2. **Efterlevnad av dataskydds- och integritetslagstiftning**

3.2.1. I den mån data kan betraktas som personuppgifter försäkrar varje part att de följer förordning (EU) 2016/679 (*allmänna dataskyddsförordningen*) och, i förekommande fall, direktiv 2002/58/EG, samt all annan tillämplig dataskyddslagstiftning.

3.2.2. Parterna måste i **tillägg 3** ange vilka data som kan betraktas som personuppgifter, samt parternas respektive skyldigheter när det gäller behandling av sådana personuppgifter enligt detta avtal.

Parternas roller och avtal enligt dataskyddsförordningen

Begreppet *personuppgifter* enligt dataskyddsförordningen är mycket brett. Det omfattar alla data som avser en identifierad eller identifierbar person. Icke-personuppgifter kan bli personuppgifter, till exempel när de ingår i en blandad datamängd, där de kombineras med nya data och resultatet av denna kombination gör det möjligt att koppla dessa data till en identifierad eller identifierbar person. Detta kan också inträffa när nya möjligheter till databehandling uppstår. Parterna bör bedöma sina egna roller enligt dataskyddsförordningen.

Viktiga begrepp i dataskyddsförordningen:

— *den registrerade*: den identifierade eller identifierbara fysiska person som uppgifterna avser.

— *personuppgiftsansvarig*: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter.

— *personuppgiftsbiträde*: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.

Dessa klausuler gäller när datadelaren är en personuppgiftsansvarig eller en gemensamt personuppgiftsansvarig med en annan part enligt dataskyddsförordningen. För att avgöra vem som har vilken roll enligt dataskyddsförordningen måste parterna överväga om de beslutar varför (ändamål) och hur (vilka medel som ska användas) personuppgifterna behandlas.

— Om datadelaren delar data med datamottagaren som använder data för egna ändamål är båda parterna separat personuppgiftsansvariga och har eget ansvar för att följa dataskyddsförordningen.

— Om datadelaren delar data med datamottagaren för att uppnå ett gemensamt ändamål är datadelaren och datamottagaren gemensamt personuppgiftsansvariga enligt artikel 26 i dataskyddsförordningen. De måste gemensamt komma överens om hur de ska följa dataskyddsförordningen.

— Om ytterligare avtalsklausuler behövs för att säkerställa efterlevnaden av dataskyddsförordningen (t.ex. enligt artikel 26 eller artikel 46) kan (och bör) sådana klausuler användas tillsammans med dessa standardavtalsvillkor. Parterna kan hänvisa till dem i **tillägg 3**, som i allmänhet bör ange hur kraven i dataskyddsförordningen uppfylls, inklusive när det gäller parternas respektive roller och ansvarsområden enligt dataskyddsförordningen.

Giltig rättslig grund

Det bör finnas en giltig rättslig grund enligt artikel 6.1 i dataskyddsförordningen för att dela data, och den registrerade måste informeras om denna (vidare) behandling enligt artikel 13 eller 14 i dataskyddsförordningen.

— En giltig rättslig grund för den som delar data och den som tar emot data i egenskap av två separat eller gemensamt personuppgiftsansvariga kan vara samtycke från den berörda personen, ett avtal med den berörda personen eller i dennes intresse eller den personuppgiftsansvariges eller tredje parts berättigade intresse (förutsatt att detta inte åsidosätts av den berörda personens intressen eller rättigheter).

— Data får endast delas för ett specificerat, uttryckligt och berättigat ändamål. Detta kan till exempel vara datadelning i syfte att förbättra produkten, där parterna har kommit överens om att använda data för att gemensamt utveckla en ny funktion.

— En datadelare som agerar som personuppgiftsansvarig kan också, på grundval av sitt berättigade intresse att bättre behålla kunder i framtiden, dela data med sitt moderbolag, som också agerar som oberoende personuppgiftsansvarig och använder data för att skapa global statistik, på grundval av sitt berättigade intresse att förbättra de tjänster som koncernen tillhandahåller globalt.

Datamottagaren bör få tillräcklig information från datadelaren för att kunna visa att den uppfyller kraven i dataskyddsförordningen. Parterna kan till exempel komma överens om att i **tillägg 3** ange det ursprungliga syftet med datainsamlingen. Detta kan vara nödvändigt för att fastställa om behandling för ett annat syfte är förenligt med det syfte för vilket personuppgifterna ursprungligen samlades in enligt artikel 6.4 i dataskyddsförordningen i fall av gemensamt personuppgiftsansvar. Alla nödvändiga detaljer om parternas respektive skyldigheter när det gäller behandling av sådana personuppgifter enligt detta avtal ska anges i **tillägg 3**.

Mer information om dataskyddsförordningen:

— Förklaring av viktiga begrepp i dataskyddsförordningen:

https://commission.europa.eu/law/law-topic/data-protection/data-protection-explained_en

— Dataskyddsguide för småföretag:

https://www.edpb.europa.eu/sme-data-protection-guide/home_sv

— Europeiska dataskyddsstyrelsens riktlinjer, rekommendationer och bästa praxis:

https://www.edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_sv

— Du kan hitta ytterligare vägledning från nationella dataskyddsmyndigheter i varje medlemsstat. Förteckning över nationella dataskyddsmyndigheter:

https://www.edpb.europa.eu/about-edpb/about-edpb/members_sv

— Standardavtalsklausuler enligt artikel 28 i dataskyddsförordningen:
https://commission.europa.eu/publications/publications-standard-contractual-clauses-sccs_en

— Information vid överföring av personuppgifter utanför EU/EES:
https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection_en

3.3. **Felaktiga uppgifter**

3.3.1. En part som får kännedom om att någon av de uppgifter som avses i denna klausul är eller inte längre är korrekta, eller inte längre kommer att vara korrekta inom överskådlig framtid, ska utan oskäligt dröjsmål underrätta den andra parten om detta, såvida inte den andra parten redan har eller borde ha kännedom om detta.

3.3.2. När den berörda parten blir medveten om denna situation måste den vidta lämpliga åtgärder och i möjligaste mån rätta till felaktigheten i uppgifterna. Om situationen inte kan rättas till måste detta avtal sägas upp genom ett skriftligt uppsägningsmeddelande där den ena parten anger skälen för uppsägningen till den andra parten. Uppsägningen träder i kraft omedelbart. Om felaktigheten endast påverkar en del av de data som omfattas av detta avtal, ska uppsägningen endast gälla den relevanta delen.

3.3.3. Ytterligare verkningar av uppsägningen regleras av klausul 9.3.

4. Tillhandahållande av data

4.1. Dataegenskaper

Datadelaren kan göra olika typer av åtaganden avseende de data som tillhandahålls, från det mest grundläggande åtagandet att de ska tillhandahållas med metadata, vilket gör dem begripliga, till det strängaste åtagandet att de ska passa de syften som datamottagaren avser och/eller vara uttömmande och korrekta. Parterna kan välja mellan följande alternativ.

Det är dessutom möjligt för parterna att lägga till ytterligare krav som är rimliga med tanke på den specifika situationen för datadelning: Till exempel när data delas för forskningsändamål kan målet om reproducerbarhet i forskningen kräva att frekvensen och lagringstiden för varje uppdaterad version av datamängden anges. I så fall kan dessa uppgifter läggas till i avsnittet ”specifika kvalitetskrav” nedan.

Datadelaren ska göra data tillgängliga för datamottagaren

(a) i samma kvalitet som de är tillgängliga för datadelaren, och

(b) tillsammans med relevanta metadata, domäntabeller, semantik, licensinformation och annan information som krävs för att göra data begripliga för datamottagaren.

[ALTERNATIV] c) [och (*välj, om tillämpligt, ett eller flera alternativ efter behov*)

i) Data görs tillgängliga i ett heltäckande, strukturerat, allmänt använt och maskinläsbart format. Parterna anser att detta krav uppfylls genom följande specifikationer avseende data: (*ange närmare*)

ii) Data görs tillgängliga i enlighet med FAIR-principerna (sökbara, tillgängliga, kompatibla och återanvändbara) som beskrivs närmare i www.go-fair.org/fair-principles: [ALTERNATIV] [(*beskriv hur FAIR-kriterierna uppfylls*)]

Efterlevnad av FAIR-principerna kan uppnås genom att uppfylla flera mätbara krav. RDA FAIR-mognadsmodellen (https://publications.jrc.ec.europa.eu/repository/handle/JRC140764) ger vägledning för att bedöma i vilken utsträckning dessa indikatorer uppfylls. En datadelare bör anpassar sina datadelningsrutiner till en mognadsnivå som är lämplig för dess specifika behov.

Datadelaren måste åtminstone se till att metadata är tillgängliga och uppfyller alla indikatorer som markerats som ”väsentliga” i mognadsmodellen. Dessutom kan en datadelare använda verktyg, god praxis och riktlinjer som är specifika för sammanhanget, till exempel de som finns tillgängliga på https://doi.org/10.2760/5646214, för att förenkla och konkretisera genomförandet av FAIR-principerna.

iii) Data är anpassade till följande sammanhang för behandling av datadelaren i enlighet med de vanliga förväntningarna: (*lägg till en kort beskrivning*)

iv) Data är lämpliga för de mål som datamottagaren eftersträvar: (*lägg till en kort beskrivning*)

v) Datadelaren ska göra följande tillgängligt för datamottagaren: (*lägg till/ta bort/komplettera specifika kvalitetskrav*)

— En uttömmande datamängd, dvs. data innehåller alla data som datadelaren förfogar över inom ramen för detta avtal, och/eller

— en uppdaterad datamängd, dvs. data återspeglar de data som datadelaren förfogar över den dag då detta avtal undertecknas, och/eller

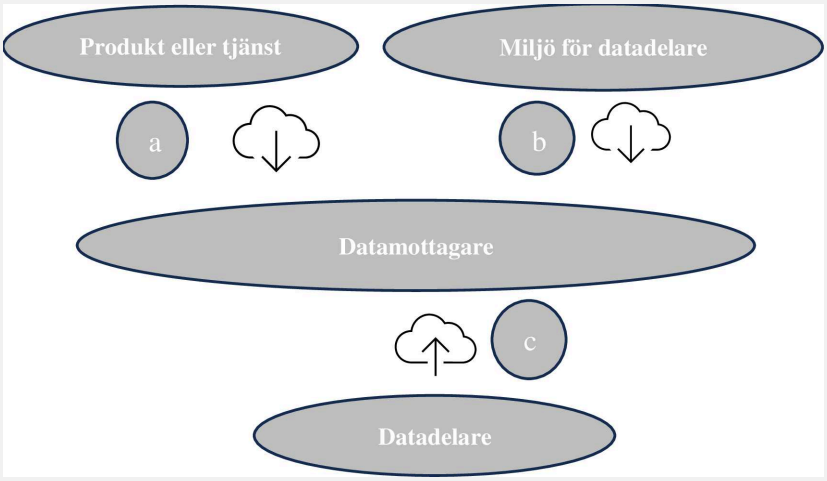
— en korrekt datamängd, dvs. att data har sammanställts av datadelaren och – såvitt denne vet – är felfria, korrekta och tillförlitliga, och/eller

— en datamängd som uppfyller följande standarder: (*ange, t.ex. interoperabilitet, tillgänglighet, säkerhet osv.*)

— En datamängd som är tillgänglig i ett öppet format, dvs. ett format som inte är proprietärt och som kan användas av vem som helst, nämligen (*ange*).]

4.2. **Datadelarens skyldigheter i samband med åtkomst till data**

Datadelaren kan göra data tillgängliga på olika sätt, antingen genom att ge eller behålla teknisk kontroll över data (utan att det påverkar de immateriella rättigheter som beviljats eller behållits). Parterna kan till exempel komma överens om att datamottagaren hämtar data från produkten eller tjänsten (alternativ a) eller från datadelarens miljö (alternativ b), eller att datadelaren överför data till datamottagarens miljö (alternativ c).



Parterna kan också komma överens om att data inte ska överföras till datamottagaren utan göras tillgängliga för behandling i datadelarens miljö. Detta skulle vara särskilt relevant i en situation som rör personuppgifter (alternativ d).



När data görs tillgängliga enligt ett eller flera av dessa alternativ måste parterna vidta olika datasäkerhetsåtgärder för att säkerställa initial och fortlöpande konfidentialitet, integritet och tillgänglighet för data. Utöver de rättsliga skyddsåtgärderna avseende personuppgifter som beskrivs i 3.2 (respektive i tillägg 3) bör säkerhetsåtgärderna (som beskrivs närmare i tillägg 4) även omfatta tekniska och organisatoriska aspekter avseende till exempel

— datakonfidentialitet genom åtkomstkontroll och säkert dataflöde,

— bestämmelser om lagring och radering av data,

— åtgärder för dataintegritet och övervakning,

— bestämmelser om dataintrång.

4.2.1. Datadelaren ska göra data tillgängliga för datamottagaren genom att

(a) [ALTERNATIV: Hämtning genom datamottagaren från produkter eller tjänster] [möjliggöra hämtning direkt från följande produkter och/eller tjänster som datadelaren inte är värd för, inklusive genom att tillhandahålla alla nödvändiga tekniska specifikationer (t.ex. kommunikationsprotokoll) under följande tekniska villkor: (*infoga metod och produkter/tjänster som inte hostas av datadelaren*),]

(b) [ALTERNATIV: Hämtning genom datamottagaren från datadelarens miljö] [möjliggöra hämtning från datadelarens miljö, inklusive genom att tillhandahålla alla nödvändiga tekniska specifikationer, under följande tekniska villkor: (*infoga metod, t.ex. nedladdning av fil eller användning av API (gränssnitt för applikationsprogrammering) för att interagera med datadelarens tjänster*),]

(Tillämpligt om alternativ a eller b väljs) [Datadelaren ger härmed datamottagaren tillstånd att använda specifikationerna för att hämta data enbart i enlighet med vad som anges i detta avtal. Med undantag för ovannämnda rättighet godkänner och bekräftar datamottagaren härmed att denne inte har någon annan rättighet till, intresse i eller licens för specifikationerna.]

(c) [ALTERNATIV: Överföring från datadelaren till datamottagarens miljö] [säkerställa fullständig överföring av data från datadelarens miljö till datamottagarens miljö, under följande tekniska villkor: *(ange metod, t.ex. engångsöverföring eller regelbundna överföringar av zip-filer till datamottagaren),*]

(d) [ALTERNATIV: Datamottagarens åtkomst till datadelarens miljö] [tillhandahålla åtkomst till data i datadelarens miljö under följande tekniska villkor: *(ange metod, t.ex. inloggning på en plattform, tillåtna funktioner inklusive exportfunktioner, beroende på vad som är tillämpligt).*]

Datadelaren ger härmed datamottagaren en icke-överlåtbar, icke-underlicensierbar rätt att få åtkomst till data i den miljö som beskrivs ovan endast för det ändamål och under den tid som anges i detta avtal. Datadelaren förbehåller sig rätten att stänga av åtkomsten till miljön om bristande efterlevnad upptäcks.

4.2.2. För tillämpningen av punkt 4.2.1 ska datadelarens miljö och datamottagarens miljö anses omfatta

(a) miljön hos tredje part som utsetts av den berörda parten att lagra eller ta emot data på deras vägnar (inklusive, i förekommande fall, säker behandlingsmiljö enligt definitionen i artikel 2.20 i förordning (EU) 2022/868),

(b) alla applikationer eller programvaror som den berörda parten tillhandahåller direkt eller via tjänsteleverantörer.

I fall där applikationer för maskininlärning eller AI ska utvecklas kan ny teknik, såsom federerad inlärning och differentiell integritet, som beskrivs närmare i https://publications.jrc.ec.europa.eu/repository/handle/JRC141298, användas för att säkerställa att datamottagaren får åtkomst till data på ett sätt som skyddar integriteten.

När det gäller federerad inlärning ”besöks” data av datamottagarens algoritm, som körs i datadelarens eller en tredje parts säkra bearbetningsmiljö. Detta tillvägagångssätt förhindrar att datamottagaren får direkt åtkomst till och insyn i data. När det gäller differentiell integritet läggs brus till originaldata för att skydda vissa känsliga egenskaper.

4.2.3. Datadelaren ska göra data tillgängliga för datamottagaren i enlighet med följande tidsfrister/kalender: (*ange tidsfrister, t.ex. dagligen, specifik tid, frekvens, realtid) och/eller detaljerad kalender eller tidsgräns*)

[ALTERNATIV] [Om datadelaren under avtalets löptid kommer i besittning av en uppdaterad eller korrigerad version av data, förbinder den sig att utan oskäligt dröjsmål göra denna uppdaterade eller korrigerade version tillgänglig för datamottagaren efter det att den blivit tillgänglig för datadelaren. Om data kontinuerligt uppdateras och korrigeras, kommer de att göras tillgängliga för datamottagaren (*ange: dagligen/veckovis/månadsvis*).]

[ALTERNATIV] Datadelaren ska se till att varje ny version av datamängden är korrekt märkt och att tidigare versioner förblir tillgängliga för mottagaren under avtalets löptid och under en period av (*ange*) därefter.

[ALTERNATIV] Data lagras av datadelaren under en period av (*ange*), varefter de inte längre är tillgängliga för datamottagaren.

4.2.4. Datadelaren måste förse datamottagaren med de medel och den information som krävs för att få åtkomst till eller ta emot data i enlighet med detta avtal. Detta omfattar särskilt

(a) [ALTERNATIV om data inte tillhandahålls i ett standardformat] [tillhandahållande av programvara och tillhörande licens som krävs för att använda data för det överenskomna ändamålet och som inte är lätt åtkomlig på marknaden men som kan tillhandahållas av datadelaren och/eller kartläggning från det tillgängliga formatet till en öppen och allmänt använd specifikation/terminologi,]

(b) tillhandahållande av information som är lätt åtkomlig för datadelaren om ursprunget till data och eventuella rättigheter som tredje part kan ha avseende data, eller omständigheter som kan ge upphov till sådana rättigheter.

[ALTERNATIV] Parterna är härmed överens om att dessa medel och denna information omfattar följande: *(ange)*.

4.3. **Datamottagarens skyldigheter i samband med åtkomst till data**

4.3.1. Datamottagaren ska förse datadelaren med den tekniska information och de relevanta data som krävs för att datadelaren ska kunna uppfylla ovanstående krav.

4.3.2. (Om tillämpligt vid åtkomst till data i datadelarens miljö) Datamottagaren

(a) ska säkerställa att endast anställda som arbetar för eller med datamottagaren och vars arbetsuppgifter kräver åtkomst för fullgörandet av detta avtal (behovsenlig behörighet) får åtkomst till datadelarens miljö och att dessa anställda följer detta avtal, dess tillägg och tillämplig lagstiftning,

(b) ska inte

i) ge någon tredje part tillstånd eller möjlighet att få åtkomst till datadelarens miljö,

ii) skapa härledda verk eller få åtkomst till datadelarens miljö för att utveckla konkurrerande produkter eller tjänster eller för att kopiera någon del, funktion eller graf i datadelarens miljö,

iii) kopiera, replikera, bakåtkompilera, dekompilera, demontera eller försöka extrahera källkod, algoritmer, metoder eller tekniska lösningar som används i datadelarens miljö [OPTION] [utom i den utsträckning som är absolut nödvändig för kompatibilitetstestning eller optimering för integration],

iv) kringgå eller förbigå säkerhetsmekanismer i datadelarens miljö, eller

v) använda datadelarens tekniska miljö för att få åtkomst till andra data än de data som omfattas av detta avtal eller under andra villkor än de villkor som anges i detta avtal.

4.4. **Säkerhetsåtgärder**

4.4.1. Varje part ska säkerställa datas konfidentialitet, integritet och tillgänglighet genom att vidta lämpliga säkerhetsåtgärder som beskrivs i **tillägg 4** när data görs tillgängliga enligt villkoren för åtkomst i 4.2.1.

4.4.2. Om förändringar i data eller deras miljö kan påverka datasäkerheten, är datadelaren och datamottagaren överens om att utvärdera säkerhetsåtgärderna (*ange: regelbundet/på begäran av den andra parten/vid särskilda händelser*) och att i god tro förhandla om nödvändiga anpassningar.

4.4.3. Varje part ska på begäran tillhandahålla den andra parten detaljerad information om de genomförandeåtgärder som vidtagits i enlighet med denna klausul 4.4 och tillägg 4.

4.4.4. Varje part ska rapportera till den andra parten alla säkerhetsöverträdelser som leder till oavsiktlig eller olaglig förstörelse, förlust, ändring, obehörigt röjande av eller obehörig åtkomst till data inom 24 timmar efter upptäckten.

4.4.5. [ALTERNATIV] [Datadelaren förbehåller sig rätten att genomföra periodiska revisioner eller begära dokumentation för att säkerställa att säkerhetskraven som åläggs datamottagaren efterlevs.]

4.4.6. *(om tillämpligt)* Datadelaren förbinder sig att inte lagra någon information om datamottagarens åtkomst till begärda data utöver vad som är nödvändigt för

(a) åtkomst till data,

(b) *(om tillämpligt)* säkerheten och underhållet av datainfrastrukturen, och

(c) efterlevnaden av de rättsliga skyldigheter som datadelaren omfattas av.

Datadelaren ska informera datamottagaren om den information som datadelaren lagrar i enlighet med tillämpliga lagar eller om datamottagaren begär det.

4.5. **Skyldighet att omförhandla, återkoppling och ensidiga ändringar**

4.5.1. Om data görs tillgängliga i enlighet med avtalsvillkoren avseende dataegenskaper, åtkomstförfaranden eller nödvändiga medel och information för att få åtkomst till och använda data, och om det framgår att de överenskomna avtalsvillkoren är otillräckliga för att få åtkomst till och använda data enligt överenskommelsen i detta avtal, åtar sig parterna att inleda förhandlingar i god tro och anpassa avtalsvillkoren.

4.5.2. Om datamottagaren identifierar en incident som rör klausul 2 om de data som omfattas av avtalet eller klausulerna 4.1 och 4.2 om dataegenskaper och villkor för åtkomst, och om datamottagaren förser datadelaren med en detaljerad beskrivning av incidenten, måste datadelaren och datamottagaren samarbeta i god tro för att identifiera orsaken till incidenten. Om incidenten orsakades av att datadelaren inte fullgjort sina skyldigheter måste denne åtgärda överträdelsen utan oskäligt dröjsmål. Om datadelaren inte gör detta anses det vara en grundläggande underlåtenhet att fullgöra sina skyldigheter, och datamottagaren kan åberopa klausul 10 i detta avtal om åtgärder vid avtalsbrott.

4.5.3. Om något av de villkor för åtkomst som överenskommits i enlighet med klausulerna 4.1 och 4.2 är omöjlig eller alltför betungande att uppnå på grund av en exceptionell förändring av omständigheterna som inträffat efter avtalets ingående, måste datadelaren tillhandahålla datamottagaren en detaljerad beskrivning av situationen och parterna ska inleda förhandlingar i god tro och anpassa avtalsvillkoren. I synnerhet måste varje part förse den andra med tillräcklig information för att bedöma, diskutera och lösa den specifika situationen. Denna klausul påverkar inte datamottagarens rätt att åberopa rättsmedel i enlighet med klausul 10.

4.5.4. Datadelaren får i god tro ensidigt ändra detaljerna i avtalsvillkoren för data och åtkomst, om detta är objektivt motiverat av datadelarens normala affärsverksamhet, till exempel genom en teknisk modifiering på grund av en omedelbar säkerhetsrisk i den produktlinje eller de tillhörande tjänster som datadelaren erbjuder eller en förändring i datadelarens infrastruktur. Alla ändringar måste uppfylla de grundläggande kraven i klausulerna 4.1 och 4.2.

4.5.5. Datadelaren måste meddela datamottagaren om ändringen minst (*ange en rimlig tidsperiod*) innan ändringen träder i kraft.

En kortare tidsfrist kan vara tillräcklig

(a) om ändringen inte påverkar datamottagarens åtkomst till och användning av data negativt, eller

(b) om ett sådant meddelande skulle vara omöjligt eller orimligt under omständigheterna, till exempel om omedelbara ändringar krävs på grund av en säkerhetsbrist som just har upptäckts.

Om ändringen påverkar datamottagarens åtkomst till och användning av data negativt, åtar sig parterna att samarbeta för att mildra sådan påverkan. Datamottagaren kan i alla händelser säga upp (den relevanta delen av) avtalet utan att någon ersättning ska betalas till datadelaren, utan att detta påverkar andra rättigheter eller rättsmedel som datamottagaren kan ha.

5. **Användning av data och delning med tredje part**

5.1. **Användning av data**

5.1.1. Godkända ändamål (*välj endast ett alternativ*)

[BEGRÄNSANDE ALTERNATIV] [Datamottagaren får endast behandla data för (*ange auktoriserade ändamål*) (*godkända ändamål*)]

eller

[BRETT ALTERNATIV endast för icke-personuppgifter] [Datamottagaren får behandla data för alla lagliga ändamål (*godkända ändamål*) [ALTERNATIV] [utom (*ange, t.ex. använda de data som erhålls för att få insikter om den ekonomiska situationen, tillgångarna och produktionsmetoderna hos eller användningen av datadelaren*)].]

(*Om tillämpligt, om data innehåller produktdata eller data från tillhörande tjänster och datadelaren enligt detta avtal har fått åtkomst till dessa i enlighet med artikel 4 eller 5 i dataförordningen i egenskap av användare eller datamottagare*) I alla händelser får datamottagaren inte använda de data som denne erhåller för att utveckla en produkt som konkurrerar med den produkt från vilken data härrör.

När parterna kommer överens om de godkända ändamålen bör de beakta eventuella begränsningar som följer av tillämplig lag eller deras avtalsenliga åtaganden gentemot tredje part. Om data exempelvis är produktdata enligt definitionen i dataförordningen och om datadelaren är en användare av produkten eller en datamottagare i den mening som avses i dataförordningen, bör de följa förbudet mot att utveckla en konkurrerande produkt enligt artiklarna 4.10 och 6.2 e i dataförordningen. Om datadelaren är en sådan användare och har kommit överens med datahållaren om särskilda begränsningar av sina lagliga rättigheter enligt dataförordningen, ska detta avtal följa sådana begränsningar.

5.1.2. Godkända åtgärder avseende data (*välj endast ett alternativ*)

[BEGRÄNSANDE ALTERNATIV] [Datamottagaren får endast vidta följande åtgärder avseende data: (*ange godkända åtgärder, t.ex. åtkomst till och kopiering av data för att skapa aggregerad statistik i relation till de godkända ändamålen*) (*godkända åtgärder*)]

eller

[BRETT ALTERNATIV endast för icke-personuppgifter] [Datamottagaren får utföra alla lagliga åtgärder på data (*godkända åtgärder*) [ALTERNATIV] [utom (*ange, t.ex. värd eller på annat sätt överföra eller göra data tillgängliga utanför Europeiska unionen, eller försöka identifiera registrerade*)]

(*Om tillämpligt, om data innehåller produktdata eller data från tillhörande tjänster och datadelaren enligt detta avtal har fått åtkomst till dessa i enlighet med artikel 4 eller 5 i förordning (EU) 2023/2854 i egenskap av användare eller datamottagare*) I alla händelser får datamottagaren inte använda de data som denne erhåller på ett sätt som negativt påverkar säkerheten för produkten eller någon tillhörande tjänst.]

5.1.3. Vidare förbinder sig datamottagaren att inte ägna sig åt följande beteenden i syfte att erhålla data:

(a) Lämna falsk information till datadelaren.

(b) Använda bedrägliga metoder eller tvångsmedel.

(c) Utnyttja luckor eller sårbarheter i datadelarens tekniska infrastruktur som är avsedd att skydda data.

5.1.4. Rätten att använda data i enlighet med denna klausul beviljas datamottagaren (*ange: på obestämd tid/under avtalets giltighetstid/under en period av (ange)*).

5.1.5. *(Om tillämpligt vid hämtning av data från/överföring av data till datamottagaren och om parterna kommer överens om en tidsbegränsning för användningen av data)* Vid upphörande eller utgång av sin rätt att använda data åtar sig datamottagaren att permanent radera data (inklusive alla kopior eller säkerhetskopior) och att säkerställa att alla tredje parter till vilka data har lämnats ut permanent raderar sådana data. Datamottagaren ska utan oskäligt dröjsmål tillhandahålla skriftligt intyg om sådan radering på begäran av datadelaren.

5.2. **Delning av data med tredje part**

5.2.1. Datamottagaren får inte dela eller överföra några data till någon tredje part, vare sig i identifierad, anonymiserad, pseudonymiserad eller aggregerad form [ALTERNATIV] [, med undantag för att datamottagaren får dela data enbart för följande användning av data: *(ange)*. Tredje part får inte dela eller överföra några data vidare [ALTERNATIV] [, med undantag för följande användning av data: (*ange*).]

5.2.2. *(om tillämpligt, om data innehåller produktdata eller data från tillhörande tjänster och datadelaren enligt detta avtal har fått åtkomst till dessa i enlighet med artikel 4 eller 5 i dataförordningen i egenskap av användare eller datamottagare)* Datamottagaren får inte göra de data som denne erhåller tillgängliga för ett företag som utsetts till grindvakt enligt artikel 3 i förordning (EU) 2022/1925 (lagen om digitala marknader).

5.2.3. Om datamottagaren har tillstånd att göra data tillgängliga för en tredje part på grundval av detta avtal, måste datamottagaren

(a) [ALTERNATIV] [informera datadelaren om att data kommer att göras tillgängliga för en tredje part, ange vilka data det rör sig om och tillhandahålla datadelaren identiteten och kontaktuppgifterna för den tredje parten,]

(b) vidta lämpliga avtalsmässiga, tekniska och organisatoriska åtgärder för att säkerställa att tredje part uppfyller samma eller i huvudsak likvärdiga skyldigheter som uppkommer för datamottagaren enligt detta avtal. Detta omfattar i synnerhet datamottagarens skyldigheter att

i) säkerställa att tredje part tillämpar minst samma säkerhetsåtgärder och skyldigheter som datamottagaren har åtagit sig enligt klausulen ”Säkerhetsåtgärder”, och

ii) säkerställa att tredje part använder data uteslutande på ett sätt som är förenligt med klausul 5.1 om användning av data, och

iii) [ALTERNATIV] [säkerställa att datadelaren har minst samma rättsmedel mot tredje part för obehörig användning eller utlämnande av data som mot datamottagaren enligt detta avtal, och]

iv) *(tillämpligt om tredje part har rätt att göra data tillgängliga för andra parter i enlighet med klausul 5.2.1)* [kräva att tredje part säkerställer att alla efterföljande tredje parter som tar emot data uppfyller de skyldigheter som anges i detta avtal].

5.2.4. Utan hinder av klausulerna 5.2.1 till 5.2.3 får datamottagaren använda behandlingstjänster, t.ex. molntjänster (inklusive infrastruktur som en tjänst, plattform som en tjänst och programvara som en tjänst), värdtjänster eller liknande tjänster för att för egen räkning och på eget ansvar använda data enligt överenskommelsen i klausulerna 5.1.1 och 5.2.1. Tredje parter får också använda sådana tjänster för att för egen räkning och på eget ansvar använda data enligt vad som avtalats i klausul 5.2.1.

6. **(om data är skyddade som företagshemligheter) Företagshemligheter**

Om företagshemligheter:

Företagshemligheter är konfidentiell information som ger ett företag en konkurrensfördel.

Enligt artikel 2.1 i direktiv (EU) 2016/943 avses med *företagshemlighet* information som uppfyller tre krav: a) Den är hemlig i den meningen att den inte, som helhet eller i den form dess beståndsdelar ordnats och satts samman, är allmänt känd hos eller lättillgänglig för personer i de kretsar som normalt sett handskas med typen av information i fråga. b) Den har kommersiellt värde på grund av att den är hemlig. c) Den person som lagligen kontrollerar den har med hänsyn till omständigheterna vidtagit rimliga åtgärder för att hålla den hemlig.

Med *innehavare av en företagshemlighet* avses en fysisk eller juridisk person som lagligen kontrollerar en företagshemlighet.

När det gäller data är datadelaren berättigad till skydd av affärshemligheter, särskilt när den digitala informationen omfattar

— teknisk information (produktteknik, FoU-data, processkunskap, opatenterad teknik m.m.),

— kommersiell information (marknadsstrategier, finansiell information m.m.).

När det gäller digital information måste datadelaren därför identifiera potentiella företagshemligheter. För mer information om företagshemligheter inom den digitala sektorn, se WIPO:s guide till företagshemligheter och innovation på

https://www.wipo.int/web-publications/wipo-guide-to-trade-secrets-and-innovation/en/part-vii-trade-secrets-and-digital-objects.html

Begränsad åtkomst för andra, kryptering eller sekretessavtal är metoder för att hålla data hemliga, vilket möjliggör skydd av företagshemligheter.

Hur hanterar man företagshemligheter?

Om datadelaren identifierar vissa företagshemligheter som en del av datadelningen enligt avtalet är den inte skyldig att dela sådana data, till skillnad från vad som anges i artikel 4.6 och artikel 5.9 i dataförordningen.

Om datadelaren beslutar att dela sådana data kan den fastställa och komma överens om krav med datamottagaren som ett villkor för att dela data som skyddas som företagshemligheter, till exempel att vidta vissa ytterligare tekniska och organisatoriska åtgärder för att bevara konfidentialiteten. Datadelaren och datamottagaren bör i **tillägg 2** som en del av avtalet inkludera alla detaljer om de data som skyddas som företagshemligheter.

6.1. **Tillämplighet av avtal om företagshemligheter**

6.1.1. De skyddsåtgärder och tillhörande rättigheter som avtalas nedan gäller uteslutande för data eller metadata som ingår i de data som datadelaren ska göra tillgängliga för datamottagaren och som skyddas som företagshemligheter (enligt definitionen i artikel 2.1 i direktivet om företagshemligheter (EU) 2016/943) och som innehas av datahållaren eller en annan innehavare av företagshemligheter (enligt definitionen i artikel 2.2 i det direktivet).

6.1.2. Data som skyddas som företagshemligheter och identiteten på innehavaren av företagshemligheter anges i **tillägg 2**.

6.1.3. De skyldigheter som anges i klausulerna 6.2 och 6.3 förblir i kraft efter avtalets upphörande, om inte parterna kommer överens om något annat.

6.2. **Skyddsåtgärder som ska vidtas av datamottagaren**

Datamottagaren ska tillämpa de skyddsåtgärder som anges i **tillägg 4** (nedan kallade *datamottagarens skyddsåtgärder*).

Parterna bör i **tillägg 4** ange alla detaljer om skyddsåtgärderna. Åtgärderna kan vara både tekniska (t.ex. kryptering, brandväggar, delad lagring osv.) och organisatoriska (t.ex. intern styrning, lämplig identitetshantering och åtkomstkontroller, involvering av en betrodd tredje part).

Eftersom åtgärderna måste vara proportionerliga kommer deras innehåll att variera beroende på vilken typ av företagshemligheter det rör sig om. Åtgärderna kommer också att bero på om i) åtkomst ska ges till den plats där data lagras eller ii) data ska överföras i sin helhet till datamottagaren. I det första fallet har datahållaren en högre grad av kontroll och kan själv tillämpa en del av skyddsåtgärderna, medan datamottagaren kan ha en lägre användningsnivå för dessa data. I vilket fall som helst måste båda parter fokusera på att uppnå de avsedda verkningarna av detta avtal.

6.3. **Skyddsåtgärder som vidtas av innehavaren av företagshemligheter**

6.3.1. Datadelaren får tillämpa de åtgärder som överenskommits i tillägg 4 för att bevara konfidentialiteten för de data som skyddas som företagshemligheter (nedan kallade *datadelarens skyddsåtgärder*).

6.3.2. Datadelaren kan också ensidigt lägga till lämpliga tekniska och organisatoriska skyddsåtgärder, om dessa inte påverkar datamottagarens åtkomst till och användning av data enligt detta avtal negativt.

6.3.3. Datamottagaren förbinder sig att inte ändra eller ta bort datadelarens skyddsåtgärder eller de åtgärder som vidtagits i enlighet med klausul 6.3.2, om inte parterna kommit överens om annat.

6.4. **Tredje part som identifierats som innehavare av företagshemligheter**

6.4.1. Datadelaren försäkrar datamottagaren att denne har alla relevanta rättigheter från tredje part som innehar företagshemligheter för att ingå detta avtal avseende data som skyddas som företagshemligheter.

6.4.2. Datamottagarens skyddsåtgärder och datadelarens skyddsåtgärder återspeglar datadelarens avtalsenliga åtaganden gentemot den ursprungliga datahållaren. Om sådana åtaganden från datadelaren gentemot den ursprungliga datahållaren utvecklas, förbinder sig datamottagaren att följa alla nya åtgärder som överenskommits mellan datadelaren och den ursprungliga datahållaren.

7. **Immateriella rättigheter**

Med *immateriella rättigheter* avses upphovsrätt (inklusive författarrättigheter (*droit d'auteur*), rättigheter till datorprogram och andra närstående rättigheter), rättigheter till mönster (inklusive registrerade mönster och mönsterskydd), varumärken, servicemärken, handels- eller företagsnamn, varumärkesnamn, domännamn och webbadresser, rättigheter till företagshemligheter, know-how och konfidentiell och icke offentliggjord information (såsom uppfinningar, oavsett om de är patenterbara eller inte), rättigheter till logotyper och patent, rätten av sitt eget slag avseende databaser och alla liknande rättigheter som erkänns enligt tillämplig lag.

De data som omfattas av detta avtal och den tillåtna användningen av datamottagaren måste regleras av detta avtal för att skydda datadelarens immateriella rättigheter, tredje parts immateriella rättigheter eller datamottagarens nya immateriella rättigheter. När det gäller datadelning är de viktigaste immateriella rättigheterna som måste beaktas vid ingåendet av ett avtal rätten av sitt eget slag i databasdirektivet och upphovsrätten.

Rätt av sitt eget slag:

Enligt artikel 43 i dataförordningen ska ”[r]ätten av sitt eget slag enligt artikel 7 i direktiv 96/9/EG […] inte tillämpas när data erhålls från eller genereras av en uppkopplad produkt eller en tillhörande tjänst som omfattas av denna förordning, särskilt med avseende på artiklarna 4 och 5 i denna förordning. Detta påverkar [dock] inte den eventuella tillämpningen av rätten av sitt eget slag enligt artikel 7 i direktiv 96/9/EG på databaser som innehåller data som inte omfattas av denna förordning, förutsatt att kraven om skydd enligt punkt 1 i den artikeln är uppfyllda (skäl 112)”.

Den rätt av sitt eget slag som databasdirektivet ger skyddar databasens upphovsman, eftersom denne är den person som gjort betydande investeringar i form av kvalitet eller kvantitet för att förvärva, verifiera eller presentera dess innehåll. Upphovsmannen kan förbjuda utdrag och återanvändning av hela innehållet i databasen eller en väsentlig del av det, bedömt kvalitativt och/eller kvantitativt. Enskilda verk eller dataelement i databasen kan, om de är originalverk, skyddas separat av upphovsrätt, även om detta skydd skiljer sig från det skydd som databasdirektivet ger.

Upphovsrätt:

Upphovsrätt är en form av immaterialrättsligt skydd som lagen ger skaparna av originalverk. Detta skydd omfattar ett brett spektrum av verk, inklusive eventuellt databasarkitektur. Observera: Upphovsrättsskyddet har inte harmoniserats fullt ut och kan därför variera mellan medlemsstaterna.

Patent:

Delning och användning av data kan leda till uppfinningar eftersom de inspirerar till nya idéer, optimerar befintlig teknik och påskyndar utvecklingen av innovativa lösningar. Uppfinningar av teknisk karaktär som är nya och innefattar innovativa steg som kan användas inom en bransch är patenterbara. Parterna bör därför reglera uppfinningar och vem som har rätt att använda dessa patenterbara resultat.

7.1. **Tidigare immateriella rättigheter**

7.1.1. Om inte annat uttryckligen anges i avtalet behåller varje part äganderätten till alla immateriella rättigheter som parterna äger eller som licensierats till dem av tredje part före eller helt oberoende av avtalets fullgörande, inklusive eventuella ändringar och/eller förbättringar av dessa (*befintliga element*). Avtalet får under inga omständigheter anses ge någon av parterna immateriella rättigheter till den andra partens befintliga element, om inte annat uttryckligen anges i avtalet.

7.1.2. *(tillämpligt om data omfattas av immateriella rättigheter) Med förbehåll för betalning av ersättning (t.ex. licensavgifter)* enligt detta avtal beviljar datadelaren härmed datamottagaren en licens som omfattar följande egenskaper under avtalets löptid: (*ange t.ex. världsomspännande, icke-exklusiv, icke-överlåtbar*) inklusive rätten att (*ange t.ex. använda, kopiera, modifiera, förbättra, underhålla*) de data som skulle omfattas av en immateriell rättighet endast i den utsträckning som är nödvändig enligt avtalet. En underlicens till datamottagarens underleverantörer är endast tillåten för ändamål som rör underleverantörsavtal och i den utsträckning de inte är oförenliga med bestämmelserna i detta avtal.

7.2. **Immateriella rättigheter till resultaten**

7.2.1. Om datamottagarens användning av data enligt detta avtal genererar konkreta arbetsprodukter som kan skyddas av immateriella rättigheter (*resultat*), enas parterna härmed om följande:

7.2.2. [ALTERNATIV 1] [Datamottagaren blir ensam ägare till alla immateriella rättigheter som rör resultaten. Endast datamottagaren får, efter eget gottfinnande, registrera eller erhålla sådana immateriella rättigheter.]

7.2.3. [ALTERNATIV 2] [Parterna ska ha gemensam och lika rätt till immateriella rättigheter till resultaten och ska ingå ett separat avtal som beskriver villkoren för utövandet av sådana rättigheter.]

7.2.4. [ALTERNATIV 3] [Datamottagaren samtycker till att, i den utsträckning som är nödvändig, överlåta till datadelaren den fullständiga juridiska och ekonomiska äganderätten till, samt alla immateriella rättigheter till, resultaten på exklusiv basis mot en ersättning som ska avtalas mellan parterna, över hela världen, under hela den tid som de immateriella rättigheterna gäller.]

7.2.5. Dessutom är parterna överens om att ytterligare licenser för resultaten ska beviljas enligt följande:

[ALTERNATIV] [(*ange den part som inte äger immateriella rättigheter till resultaten*) beviljar härmed (*ange ägaren av immateriella rättigheter till resultaten*), under immateriella rättigheters skyddsperiod, en fullt betald, världsomspännande, icke-exklusiv, icke-överlåtbar licens att använda, kopiera, modifiera, förbättra och underhålla dess befintliga element enbart i den utsträckning som är nödvändig för att utöva sina rättigheter till resultaten enligt denna klausul.]

[ALTERNATIV] [(ange ägaren av immateriella rättigheter till resultaten) beviljar härmed (ange den part som inte äger immateriella rättigheter till resultaten), under den tid som immateriella rättigheter skyddas, en fullt betald, världsomspännande, icke-exklusiv, icke-överlåtbar licens att använda, kopiera, modifiera, förbättra och underhålla resultaten enbart för följande ändamål: (*fyll i enligt vad som är tillämpligt*).]

8. **Ersättning för tillhandahållande av dataåtkomst**

Parterna kan i själva avtalet eller i ett separat tillägg fastställa detaljer om ersättning, inklusive kostnader för att upprätta API (som används för delning av data) eller andra kostnader i samband med att underlätta delning av data, inklusive eventuella royaltyer eller licensavgifter, beroende på vad som är tillämpligt. Parterna bör åtminstone komma överens om ersättningsbeloppet och relevant valuta, tidpunkt för betalning och betalningsförfaranden.

De kan komma överens om ytterligare ersättning, i förekommande fall, för tilläggstjänster, som kommer att omfattas av en extra avgift.

Parterna är överens om att datamottagaren ska ersätta datadelaren enligt följande: (*fyll i efter behov*)

Parterna bör åtminstone komma överens om ersättningsbeloppet och relevant valuta, tidpunkt för betalning och betalningsförfaranden.

9. **Datum för tillämpning, avtalets löptid och uppsägning**

9.1. **Datum för tillämpning och löptid**

9.1.1. Detta avtal [ALTERNATIV 1] [träder i kraft omedelbart] [ALTERNATIV 2] [träder i kraft från och med den (*ange datum*)].

9.1.2. [ALTERNATIV] [Detta avtal ingås för [ALTERNATIV 1] [obestämd tid] [ALTERNATIV 2] [en fast period på (*ange*)], med förbehåll för eventuella skäl för upphörande eller uppsägning enligt detta avtal.]

9.1.3. [ALTERNATIV] [Datadelaren måste börja göra data tillgängliga för datamottagaren [ALTERNATIV 1] utan oskäligt dröjsmål efter det att avtalet har trätt i kraft. [ALTERNATIV 2] den (*ange datum och, i förekommande fall, ytterligare uppgifter om tidpunkten*).]

Om begäran avser en engångsleverans av data är det tillräckligt att komma överens om tillämpningsdatumet i klausul 9.1.1. Om begäran avser en kontinuerlig leverans av data måste parterna komma överens om avtalets löptid och välja antingen det första eller det andra alternativet i klausul 9.1.2.

9.2. **Uppsägning av praktiska skäl**

9.2.1. Datamottagaren kan säga upp avtalet när som helst under avtalsperioden genom att meddela datadelaren (*ange period*).

9.2.2. [ALTERNATIV] Om datamottagaren säger upp avtalet enligt klausul 9.3.1 före (*ange tidpunkt eller minsta avtalsperiod*), måste denne ersätta datadelaren för de kostnader som datadelaren har haft för att göra data tillgängliga, inklusive, i förekommande fall, tillhandahållande av ytterligare support, enligt följande: *(ange)*.

Det kan förekomma fall där datadelaren har kostnader för att göra data tillgängliga för datamottagaren, till exempel genom att anpassa sin digitala infrastruktur, i förvissning om att dessa kostnader kommer att amorteras över tid.

I detta fall kan datadelaren vilja säkerställa att denne får ersättning från datamottagaren.

9.3. **Verkningar av upphörande eller uppsägning**

9.3.1. När avtalsperioden löper ut eller detta avtal sägs upp befrias båda parter från sin skyldighet att utföra och ta emot framtida prestationer, men detta påverkar inte de rättigheter och skyldigheter som har uppkommit fram till tidpunkten för uppsägningen.

Upphörande eller uppsägning påverkar inte någon bestämmelse i detta avtal om tvistlösning enligt klausul 11.6 eller någon annan bestämmelse som ska gälla även efter det att avtalet har upphört.

9.3.2. [ALTERNATIV 1] [Datadelaren måste vidta lämpliga åtgärder för att underlätta utträde, såsom datamottagaren rimligen kan förvänta sig.] [ALTERNATIV 2] [Datadelaren måste vidta följande åtgärder för att underlätta utträde: (ange).]

Parterna kan överväga om datamottagaren behöver några åtgärder för att underlätta utträde.

Detta är till exempel relevant om datamottagaren hade tillåtelse att extrahera data från ett medium som kontrolleras av datadelaren men ännu inte hade extraherat data, eftersom datamottagaren inte förväntade sig att avtalet skulle sägas upp.

10. **Åtgärder vid avtalsbrott**

10.1. **Fall av underlåtenhet att fullgöra sina skyldigheter**

10.1.1. Underlåtenhet att fullgöra en skyldighet är av grundläggande betydelse om

(a) underlåtenheten väsentligen berövar den andra parten det som den hade rätt att förvänta sig enligt detta avtal, såvida inte den part som underlåtit att fullgöra sina skyldigheter inte kunde förutse och rimligen inte kunde ha förutsett detta resultat, eller

(b) det av omständigheterna framgår att man i framtiden inte kan förlita sig på den part som underlåtit att fullgöra sina skyldigheter.

10.1.2. En parts underlåtenhet är ursäktlig om den beror på ett hinder utanför dess kontroll och den parten rimligen inte kunde förväntas ta hänsyn till hindret vid tidpunkten för ingåendet av detta avtal, eller undvika eller övervinna hindret eller dess konsekvenser.

Om hindret endast är tillfälligt ska underlåtenheten vara ursäktad för den period som hindret består. Om förseningen dock innebär en grundläggande underlåtenhet att fullgöra sina skyldigheter, kan den andra parten behandla den som sådan.

Den part som underlåter att fullgöra sina skyldigheter måste se till att den andra parten utan oskäligt dröjsmål får kännedom om hindret och dess inverkan på partens förmåga att fullgöra sina skyldigheter, efter det att den part som underlåter att fullgöra sina skyldigheter har fått kännedom om eller rimligen kunde förväntas ha fått kännedom om dessa omständigheter. Den andra parten har rätt till skadestånd för ekonomisk skada som uppstår till följd av att ett sådant meddelande inte mottagits.

10.2. **Rättsmedel vid avtalsbrott**

10.2.1. Om en part inte fullgör sina skyldigheter, ska den andra parten ha de rättsmedel som anges i följande klausuler, utan att det påverkar de rättsmedel som finns tillgängliga enligt tillämplig lag.

10.2.2. Rättsmedel som inte är sinsemellan oförenliga får kombineras.

10.2.3. En part får inte utnyttja ett rättsmedel i den mån det orsakar den andra partens underlåtenhet att fullgöra sina skyldigheter, till exempel om en brist i den egna datainfrastrukturen har gjort det omöjligt för den andra parten att fullgöra sina skyldigheter. En part får inte heller åberopa ett skadeståndsanspråk i den mån den kunde ha minskat skadan genom att vidta rimliga åtgärder.

10.2.4. Den skadelidande parten kan

(a) säga upp detta avtal med omedelbar verkan utan påföljd genom att meddela den andra parten, om

i) den andra partens underlåtenhet att fullgöra sina skyldigheter är en grundläggande underlåtenhet, eller

ii) i fall av en underlåtenhet som inte är grundläggande, den skadelidande parten har meddelat att underlåtenheten måste åtgärdas utan oskäligt dröjsmål och den andra parten inte har gjort detta,

(b) kräva skadestånd för ekonomisk skada som den andra parten har orsakat genom underlåtenhet att fullgöra sina skyldigheter och som inte är undantagen enligt klausul 10.1.2; den part som underlåter att fullgöra sina skyldigheter är endast ansvarig för skador som den förutsåg eller rimligen kunde ha förutsett vid tidpunkten för ingåendet av detta avtal som ett troligt resultat av sin underlåtenhet att fullgöra sina skyldigheter, såvida inte underlåtenheten var uppsåtlig eller grovt vårdslös,

(c) begära att den part som inte fullgör sina skyldigheter utan oskäligt dröjsmål fullgör sina skyldigheter enligt detta avtal, såvida detta inte är olagligt eller omöjligt eller om specifikt fullgörande skulle medföra kostnader för den part som inte fullgör sina skyldigheter som är oproportionerliga i förhållande till den fördel som den andra parten skulle erhålla.

10.2.5. [ALTERNATIV] [Om en part underlåter att fullgöra sina skyldigheter enligt detta avtal ska den i alla fall betala de straffavgifter som anges i detalj i tillägg 5, vilka parterna anser vara skadestånd i den mening som avses i klausul 10.2.4 b. Den part som underlåter att fullgöra sina skyldigheter har rätt att begära att straffavgiften sänks till ett rimligt belopp om parten kan bevisa att straffavgiften är grovt överdriven i förhållande till den skada som uppstått till följd av underlåtenheten.

11. **Allmänna bestämmelser**

11.1. **Konfidentialitet**

11.1.1. Följande information ska betraktas som konfidentiell:

(a) Information som avser företagshemligheter, ekonomisk situation eller andra aspekter av den andra partens verksamhet, såvida inte den andra parten har offentliggjort denna information.

(b) Information som anger grunden för beräkningen av rimlig ersättning.

(c) Information som avser tredje part, såvida de inte redan har offentliggjort denna information.

11.1.2. Båda parterna är överens om att vidta alla rimliga åtgärder för att på ett säkert sätt lagra och behandla den information som avses i klausul 11.1.1 konfidentiellt och att inte lämna ut eller göra sådan information tillgänglig för tredje part, såvida inte

(a) en av parterna har en laglig skyldighet att lämna ut eller göra relevant information tillgänglig, eller

(b) det är nödvändigt för en av parterna att lämna ut eller göra relevant information tillgänglig för att fullgöra sina skyldigheter enligt detta avtal, eller

(c) en av parterna har erhållit förhandsgodkännande från den andra parten eller den part som tillhandahåller den konfidentiella informationen eller som påverkas av dess utlämnande.

11.1.3. Dessa skyldigheter avseende konfidentialitet gäller även efter avtalets upphörande under en period av (*ange period*).

11.1.4. Dessa skyldigheter avseende konfidentialitet upphäver inte strängare förpliktelser enligt i) förordning (EU) 2016/679 (allmänna dataskyddsförordningen), ii) bestämmelserna om genomförande av direktiv 2002/58/EG eller direktiv (EU) 2016/943, eller iii) annan unionsrätt eller nationell rätt.

11.2. **Kommunikationsmedel**

Alla meddelanden eller annan kommunikation som krävs eller tillåts enligt detta avtal måste vara skriftliga och kan levereras personligen, skickas med förbetald post eller överföras elektroniskt, inklusive e-post, förutsatt att avsändaren behåller bevis på att de har skickats till nedanstående adresser:

Part	Kontaktperson	E-post	Telefon	Adress
Användare	[Namn]/[Befattning]	[E-post]	[Telefon]	[Adress]
Datamottagare	[Namn]/[Befattning]	[E-post]	[Telefon]	[Adress]

Sådana meddelanden eller kommunikationer ska anses ha mottagits

(a) om de levereras personligen, på leveransdagen,

(b) om de skickas med förbetald post, den tredje arbetsdagen efter att de postats,

(c) om de skickas elektroniskt, på överföringsdagen, förutsatt att avsändaren inte har mottagit något felmeddelande som indikerar att leveransen misslyckats.

11.3. **Hela avtalet, ändringar och avskiljbarhet**

11.3.1. Detta avtal (tillsammans med dess tillägg som hänvisas till i avtalet) utgör hela avtalet mellan parterna avseende avtalets innehåll och ersätter med avseende på innehållet alla tidigare muntliga eller skriftliga avtal eller överenskommelser och uppgörelser mellan parterna avseende avtalets innehåll.

11.3.2. Alla ändringar av detta avtal är endast giltiga om de har godkänts skriftligen av parterna, inklusive i elektronisk form.

11.3.3. Om någon bestämmelse i detta avtal av någon anledning befinns vara ogiltig, upphävbar eller icke verkställbar, och om denna bestämmelse kan avskiljas från de återstående villkoren i avtalet, ska de övriga bestämmelserna inte påverkas av detta och fortsätta att vara giltiga och verkställbara, såvida inte bestämmelsen inte kan skiljas från övriga bestämmelser i detta avtal. Eventuella luckor eller oklarheter i detta avtal ska hanteras i enlighet med klausul 11.5.

11.4. **Tillämplig lag**

Detta avtal regleras av lagen i (*ange medlemsstat*).

11.5. **Tolkning**

11.5.1. Alla bestämmelser i detta avtal ska tolkas så att de överensstämmer med unionsrätt eller nationell lagstiftning som antagits i enlighet med unionsrätten, samt all tillämplig nationell rätt som är förenlig med unionsrätten och som inte kan frångås genom avtal.

11.5.2. Om någon lucka eller oklarhet i detta avtal inte kan lösas på det sätt som anges i klausul 11.5.1, ska detta avtal tolkas mot bakgrund av de tolkningsregler som föreskrivs i tillämplig lag (se klausul 11.4).

11.6. **Tvistlösning**

11.6.1. Parterna är överens om att göra sitt yttersta för att lösa tvister i godo och, innan de väcker talan vid domstol, att hänskjuta tvisten till [ange namn och kontaktuppgifter för ett särskilt tvistlösningsorgan].

11.6.2. [ALTERNATIV] [Domstolarna i (*ange medlemsstat*) har exklusiv behörighet att pröva mål som rör detta avtal.]

Tillägg 1 innehåller en beskrivning av data

[ska utarbetas av parterna]

Tillägg 2 innehåller ytterligare uppgifter om data som omfattas av en ordning som kräver särskilda åtgärder

[ska utarbetas av parterna]

Tillägg 3 innehåller detaljer om personuppgifter och parternas respektive skyldigheter

[ska utarbetas av parterna]

Tillägg 4 innehåller tillämpliga säkerhetsåtgärder för delning av data

[ska utarbetas av parterna]

[ALTERNATIV] Tillägg 5 innehåller detaljer om påföljder

[ska utarbetas av parterna]

BILAGA VI

STANDARDAVTALSKLAUSULER

om byte och utträde

De primära målen med förordning (EU) 2023/2854 (nedan kallad *dataförordningen*) om byte av molntjänster är att göra det möjligt för kunder till databehandlingstjänster (molntjänster och edgetjänster) att i) byta mellan leverantörer som erbjuder samma tjänstetyp, ii) byta till en lokal IKT-infrastruktur eller iii) använda flera tjänster från olika leverantörer samtidigt. I dataförordningen specificeras därför leverantörers och kunders rättigheter och skyldigheter i samband med denna process. I detta sammanhang bör kunderna också utvärdera sina mål i samband med byte och i synnerhet specifika behov, ytterligare utgifter eller tidpunkt. Både den ursprungliga leverantören, kunden och destinationsleverantören måste samarbeta i god tro för att göra bytesprocessen effektiv, möjliggöra en snabb överföring av data och bibehålla databehandlingstjänsternas kontinuitet (artikel 27 i dataförordningen).

Dessa standardavtalsklausuler tolkar de nya rättigheter och skyldigheter som införs genom dataförordningen när det gäller byte och utträde till avtalsvillkor. Dataförordningen kräver att leverantörer tillhandahåller kunderna ett skriftligt avtal som anger villkoren för bytet. Avtalet måste också ange tidsfrister för bytet (högst 30 dagars övergångsperiod) och detaljer om eventuella kostnader (inklusive straffavgifter för förtida uppsägning, standardavgifter för tjänster (artikel 29.4 i dataförordningen) och uttagsavgifter). Det finns också skyldigheter i samband med själva bytet som bör anges i avtalet, såsom att ge rimligt bistånd till kunden (och eventuella tredje parter som kunden har bemyndigat), upprätthålla driftskontinuiteten och säkerställa en hög säkerhetsnivå under hela bytet.

Bytesavgifter

Enligt artikel 29 i dataförordningen kan en leverantör ta ut bytesavgifter fram till den 12 januari 2027, men dessa får inte överstiga de kostnader som leverantören har direkt i samband med bytesprocessen. För byte efter den 12 januari 2027 får leverantören inte ta ut bytesavgifter. Bytesavgifterna omfattar uttagsavgifter och andra kostnader för åtgärder som leverantören är skyldig att vidta som en del av bytesprocessen. Detta omfattar till exempel kostnader för användning av automatiserade bytesverktyg eller testverktyg, om leverantören använder sådana verktyg för att fullgöra sina skyldigheter enligt dataförordningen.

Om en databehandlingstjänst används parallellt med en annan databehandlingstjänst får leverantörerna – även efter den 12 januari 2027 – fortsätta att överföra kostnaderna för datauttag till kunden (artikel 34 i dataförordningen).

I dataförordningen definieras *bytesavgifter* som avgifter ”som en leverantör av databehandlingstjänster tar ut av en kund för de åtgärder som föreskrivs i denna förordning för att byta till en annan leverantörs system eller till lokal IKT-infrastruktur […]”. I artikel 25.2 a i i dataförordningen anges också att leverantören måste ”ge kunden och tredje parter som kunden har godkänt rimligt bistånd i bytesprocessen”. Eventuella avgifter i samband med tillhandahållandet av ett sådant ”rimligt bistånd” bör avskaffas över tid, såsom anges i artikel 29.

Dataförordningen anger fall där en standardiserad metod inte är möjlig:

— Artikel 29.5: ”I förekommande fall ska leverantörer av databehandlingstjänster tillhandahålla information till en kund om databehandlingstjänster som inbegriper mycket komplexa eller kostsamma byten eller för vilka det är omöjligt att byta utan betydande störningar i data, digitala tillgångar eller tjänstearkitektur.”

— Artikel 29.6: ”I tillämpliga fall ska leverantörerna […] göra den information som avses […] allmänt tillgänglig […].”

Andra standardavtalsklausuler som rekommenderas av kommissionen finns bifogade och omfattar andra specifika teman än byte och utträde. Parterna uppmuntras att överväga att använda även dessa andra klausuler, eftersom de har utformats för att vara samstämmiga och förstärka varandra.

Särskild ordning

Det är värt att notera att artikel 31 i dataförordningen innehåller vissa undantag från vissa skyldigheter som rör standardavtalsklausulerna om byte och utträde. En särskild ordning gäller till exempel för byte av databehandlingstjänster om

(a) de flesta av databehandlingstjänstens huvudfunktioner har skapats speciellt för en enskild kunds behov ELLER alla komponenter har utvecklats för en enskild kunds ändamål och

(b) dessa databehandlingstjänster inte erbjuds i bred kommersiell skala via leverantörens tjänstekatalog, och
(c) leverantören har vederbörligen informerat kunden om att skyldigheterna vid byte inte gäller för just denna tjänst.

Beroende på det specifika undantaget kan vissa rättsliga skyldigheter inte vara tillämpliga. Det åligger dock kunden och leverantören att komma överens om huruvida dessa undantag ska inkluderas i deras avtal. Även om dessa standardavtalsklausuler inte har utformats för att täcka sådana situationer, kan de ändå tjäna som inspiration för parterna i en överenskommelse/ett avtal som rör sådana tjänster.

Leverantören bör, i god tid före ingåendet av en överenskommelse, informera potentiella kunder om specifika tjänster som omfattas av den särskilda ordning som fastställs i artikel 31 i dataförordningen.

Ingenting hindrar leverantören från att så småningom införa sådana tjänster i stor skala, i vilket fall leverantören skulle behöva uppfylla alla skyldigheter för byte som fastställs i dataförordningen.

Metoder för byte

Allt fler leverantörer erbjuder självbetjäningsverktyg för byte både för datainmatning, när kunderna börjar använda en tjänst, och datauttag, när kunderna slutar använda en tjänst och byter till antingen ett lokalt system eller en ny (destinations)leverantör. För vissa databehandlingstjänster finns det kanske inte sådana verktyg, eller så möjliggör de inte ett fullständigt byte.

I dessa standardavtalsklausuler anges två metoder för planering och genomförande av bytet, nämligen
(a) byte baserat på bytes- och utträdesplanen (alternativ A) och
(b) byte med hjälp av automatiserade verktyg (alternativ B).

Dessa alternativ kan kombineras. I **tillägg 1**, ”Bytes- och utträdesplan”, kan parterna till exempel också överväga att använda automatiserade verktyg som kan tillämpas för vissa typer av tjänster eller vissa data.

Enligt båda metoderna är leverantörerna skyldiga att undanröja hinder för effektivt byte enligt förordning (EU) 2023/2854, enligt vilken leverantörerna ”ska förse kunden med information om tillgängliga förfaranden för byte och portering till databehandlingstjänsten, inbegripet information om tillgängliga metoder och format för byten och portering samt tekniska och andra begränsningar som leverantören av databehandlingstjänster känner till” (artikel 26a), och ”[d]en ursprungliga leverantören av databehandlingstjänster ska underlätta bytesprocessen genom att tillhandahålla kapacitet, adekvat information, dokumentation, tekniskt stöd och, vid behov, nödvändiga verktyg” (artikel 30).

Det bör också noteras att leverantören inte förväntas dela eller lista några data som är specifika för den interna funktionen av leverantörens databehandlingstjänst om det finns risk för överträdelse med avseende på leverantörens företagshemligheter. Enligt de avtalsenliga skyldigheter som fastställs i artikel 25.2 f är leverantören endast skyldig att tillhandahålla en uttömmande specifikation av kategorier av sådana data.

Är standardavtalsklausulerna tillämpliga på alla modeller av molntjänster (t.ex. på IaaS-, PaaS- eller SaaS-avtal)?

Dessa standardavtalsklausuler är tillämpliga på alla typer av modeller för molntjänstavtal, där molntjänsten i fråga uppfyller definitionen av en databehandlingstjänst enligt artikel 2.8. Enligt den artikeln är en databehandlingstjänst ”en digital tjänst som tillhandahålls en kund och som möjliggör allmän nätverkstillgång på begäran till en gemensam pool av konfigurerbara, skalbara och elastiska databehandlingsresurser av centraliserad, distribuerad eller mycket distribuerad art och som snabbt kan tillhandahållas och levereras med minsta möjliga administration eller interaktion med tjänsteleverantören”. Bestämmelserna i dataförordningen gäller således för tjänstetyper som uppvisar de egenskaper som anges i definitionen av databehandlingstjänster:

— De möjliggör åtkomst till databehandlingsresurser, inklusive nätverk, servrar, lagring, applikationer och tjänster.

— De möjliggör nätverksåtkomst på begäran, vilket innebär att en kund ensidigt kan tillhandahålla dessa databehandlingsresurser som är tillgängliga via nätverket och genom standardmekanismer, till exempel via mobiltelefoner, bärbara datorer eller arbetsstationer.

— De kan snabbt tillhandahållas och frigöras med minimal förvaltningsinsats eller interaktion med tjänsteleverantören, vilket innebär att det ensidiga tillhandahållandet kan ske utan betydande ingripande från tjänsteleverantören och kan implementeras snabbt, så att organisationer kan börja använda resurserna nästan omedelbart.

— De är elastiska och kan snabbt tillhandahållas, vilket innebär att lösningarna enkelt kan skalas för att anpassas till förändrade behov och att användarna kan uppgradera eller nedgradera efterfrågan utifrån sina behov.

En leverantör vars tjänsteutbud uppvisar dessa egenskaper måste följa bestämmelserna i dataförordningen för att möjliggöra byte mellan databehandlingstjänster. Detta omfattar till exempel att anpassa tjänsteavtal till artikel 25, minska och ta bort bytes- och uttagsavgifter i enlighet med artikel 29 och följa de tekniska aspekter av byte som definieras i artikel 30. Alla krav som ställs på databehandlingstjänster enligt kapitel VI i dataförordningen gäller dock inte för SaaS. Det är särskilt viktigt att notera att begreppet *funktionell likvärdighet* i artikel 30.1 endast gäller leverantörer av IaaS, medan artiklarna 30.2 och 30.3 gäller leverantörer av PaaS och SaaS. De två sistnämnda bestämmelserna kräver att leverantörer av PaaS och SaaS tillhandahåller öppna gränssnitt och följer öppna specifikationer för interoperabilitet och harmoniserade standarder som publiceras i ett EU-register.

I artikel 30 i dataförordningen görs åtskillnad mellan

1. IaaS, som definieras som ”databehandlingstjänster som avser skalbara och elastiska datorresurser begränsade till infrastrukturella element såsom servrar, nät och de virtuella resurser som krävs för driften av infrastrukturen, men som inte ger åtkomst till de operativa tjänster, den programvara och de applikationer som lagras, på annat sätt behandlas eller används på dessa infrastrukturkomponenter”

och

2. andra typer av molntjänster.

Vidare anges i skäl 81 i dataförordningen att det generiska begreppet *databehandlingstjänster* omfattar ett stort antal tjänster med ett mycket brett spektrum av olika syften, funktioner och tekniska konfigurationer, och att de vanligtvis anses falla inom en eller flera av de tre modellerna för tillhandahållande av databehandlingstjänster, dvs. IaaS, PaaS och SaaS.

Parternas kapacitet

I artikel 24 i dataförordningen klargörs följande: ”Ansvaret för leverantörer av databehandlingstjänster enligt artiklarna 23, 25, 29, 30 och 34 ska endast gälla de tjänster, avtal eller affärsmetoder som tillhandahålls av den ursprungliga leverantören av databehandlingstjänster.”

Bland annat krävs kunskap om datastrukturen och relationen mellan data för att definiera sekvensen av åtgärder för export av exporterbara data. Nedanstående lista ger därför allmän vägledning till parterna för att hjälpa dem att förstå varandras kapacitet som ligger till grund för olika delar av bytet. Listan är dock endast vägledande, och det finns viktiga nyanser som kan skilja sig mellan och inom tjänstemodellkategorierna nedan, beroende på den specifika databehandlingstjänsten i fråga. Parterna bör vara uppmärksamma på sådana skillnader.

Infrastruktur som en tjänst (IaaS)

— Kunden känner till strukturen på den databas som denne har definierat. IaaS-leverantören känner inte till databasens struktur. IaaS-leverantören kan ge detaljerade uppgifter om porteringsmetoderna och, i förekommande fall, de nödvändiga verktygen.

— Kunden kan definiera sekvensen av åtgärder, ett tidsfönster och de it-resurser som krävs.

— Leverantören kan bekräfta tillgängligheten av de nödvändiga it-resurserna under tidsfönstret.

— Kunden kan inleda bytet vid den överenskomna tidpunkten.

— Kunden ansvarar för att importera data till destinationsmiljön och implementera dem där.

Plattform som en tjänst (PaaS)

— Kunden känner till strukturen på den databas som denne har definierat.

— PaaS-leverantören känner också till databasens egenskaper eftersom kunden har bett leverantören att tillhandahålla tjänster såsom utrymmesallokering, optimering, omorganisation och säkerhetskopiering.

— PaaS-leverantören har praktisk erfarenhet av förfaranden för åtgärder såsom säkerhetskopiering. Leverantören känner till vilka resurser som krävs och hur lång tid det tar. PaaS-leverantören kan ge detaljerade uppgifter om porteringsmetoderna och, i förekommande fall, de nödvändiga verktygen och information om tidpunkten och de it-resurser som krävs.

— Kunden kan definiera sekvensen av åtgärder, ett tidsfönster (en period, till exempel en helg, under vilken kunden avser att göra sina system otillgängliga för användarna och ingen uppdatering sker så att data fryses och kunden kan genomföra bytet) och de it-resurser som krävs.

— Leverantören kan bekräfta tillgängligheten av de nödvändiga it-resurserna under tidsfönstret.

— Kunden inleder bytet vid den överenskomna tidpunkten.

Programvara som en tjänst (SaaS)

— Kunden känner inte till databasens struktur.

— SaaS-leverantören känner till strukturen på den databas som denne har definierat.

— SaaS-leverantören känner till de förfaranden och den tid som krävs för åtgärder som säkerhetskopiering, optimering och omorganisation.

— Vid installation av en ny version av SaaS-programvaran med en ny version av databasstrukturen är det inte ovanligt att göra en fullständig export från den gamla strukturen följt av en fullständig import till den nya strukturen. Detta förfarande ger SaaS-leverantören en praktisk bild av förfarandet, resurserna och den tid som krävs för att exportera data.

— SaaS-leverantören kan ge detaljerade uppgifter om porteringsmetoderna och, i förekommande fall, de nödvändiga verktygen.

— Leverantören kan ge information om tidpunkten och de it-resurser som krävs.

— Leverantören kan föreslå exportmetoder och format samt sekvensen av åtgärder.

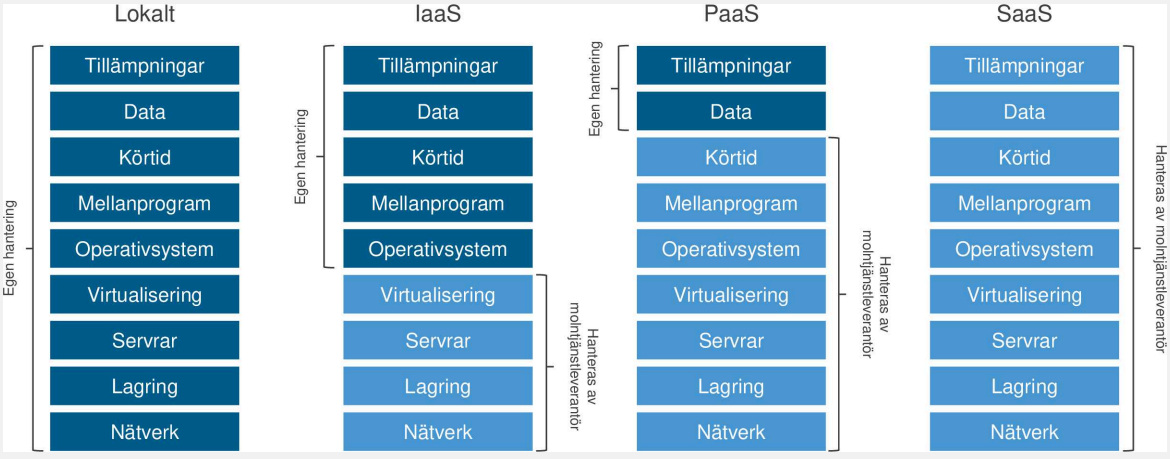
— Kunden ansvarar för att importera data i destinationsmiljön och kan ha krav och synpunkter på den föreslagna sekvensen.

— SaaS-leverantören och kunden kan komma överens om sekvensen av åtgärder, tidsfönstret och de it-resurser som krävs.

— Leverantören kan bekräfta tillgängligheten av de nödvändiga it-resurserna under tidsfönstret.

— Beroende på vilket verktyg och vilken sekvens som avtalats inleder leverantören eller kunden bytet vid den överenskomna tidpunkten.

— Kunden ansvarar för att importera data till destinationsmiljön.



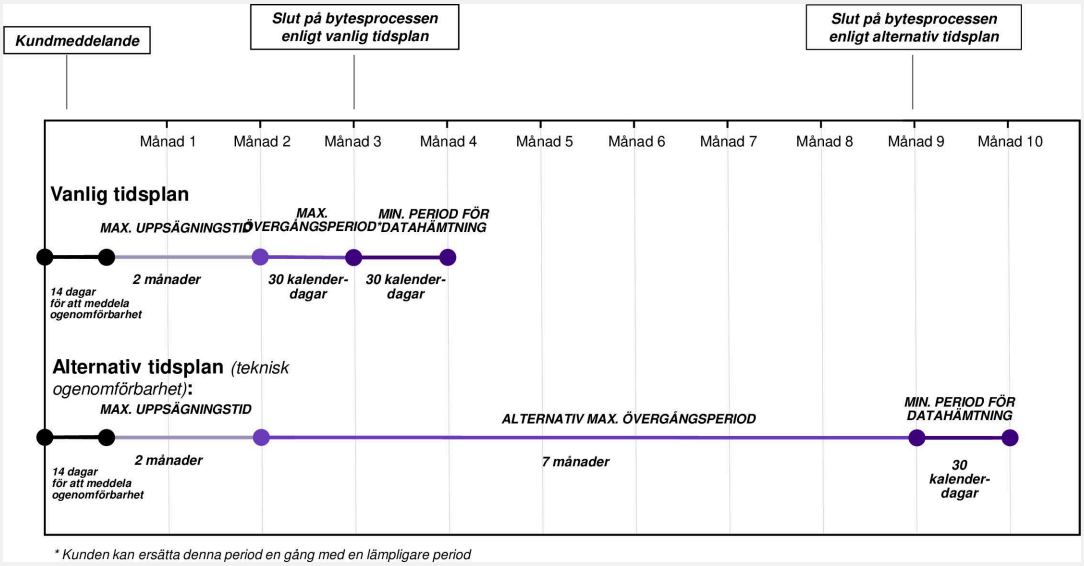
Åtgärder under den maximala uppsägningstiden och övergångsperioden

Inledande av byte: Artikel 25.2 d i dataförordningen kräver att avtalen innehåller en maximal uppsägningstid för att inleda bytesprocessen, som inte får överstiga två månader. I denna klausul anges vilken information leverantören ska lämna till kunden under denna period och vilka åtgärder leverantören ska vidta efter att bytesprocessen har inletts.

Övergångsperiod: Artikel 25.2 a i dataförordningen kräver att avtalen innehåller bestämmelser om att kunden på begäran ska kunna byta till en annan databehandlingstjänst eller överföra alla exporterbara data till lokal IKT-infrastruktur utan oskäligt dröjsmål och under alla omständigheter inom den obligatoriska maximala övergångsperioden på 30 kalenderdagar från och med utgången av den maximala uppsägningstiden.

Artikel 25.2 g i dataförordningen kräver också att avtalet innehåller en minimitid för datahämtning på minst 30 kalenderdagar, som börjar efter utgången av den övergångsperiod som parterna har kommit överens om.

Om den obligatoriska maximala övergångsperioden på 30 dagar för byte är tekniskt ogenomförbar måste leverantören underrätta kunden inom 14 arbetsdagar efter det att begäran om byte har gjorts, förklara den tekniska ogenomförbarheten och ange en alternativ övergångsperiod, som inte får överstiga sju månader (artikel 25.4 i dataförordningen). Kunden har rätt att förlänga den obligatoriska maximala övergångsperioden en gång, med en period som kunden anser vara mer lämplig (artikel 25.5 i dataförordningen).



Databehandlingsavtalet anses upphöra när bytet har genomförts eller vid utgången av den maximala uppsägningstiden, om kunden inte vill byta leverantör utan radera sina exporterbara data och digitala tillgångar när tjänsten upphör. Inget uppsägningsmeddelande från kunden behövs, eftersom avtalet upphör automatiskt. För att uppnå rättssäkerhet och säkerställa att parternas intressen skyddas är leverantören dock skyldig att underrätta kunden om avtalets upphörande (artikel 25.2 c i dataförordningen).

Alternativ A: Bytes- och utträdesplan som bilaga till avtalet

Innan avtalet ingås kan parterna överväga att utarbeta en detaljerad bytes- och utträdesplan. Detta kan vara särskilt användbart vid komplexa databehandlingstjänster. Den bytes- och utträdesplan som ingår här ger parterna en tydlig bild från början av avtalsförhållandet avseende bytesprocessen, inklusive vilken typ av information, data och processer som behöver delas mellan parterna för att bytet ska kunna ske utan fördröjning eller påverkan på kundens tjänster eller verksamhet.

Mallen för en ”bytes- och utträdesplan” i **tillägg 1** är endast ett exempel på en sådan plan som ger kunden en uppfattning om de frågor som de behöver ställa till sin leverantör och om strukturen för dessa diskussioner.

Ansvarsfördelningen under genomförandet av bytesprocessen är ett exempel som, där så är relevant, är anpassat till de rättigheter och skyldigheter som fastställs i dataförordningen. Med respekt för dessa rättigheter och skyldigheter kan parterna komma överens om en annan fördelning eller om att inkludera ytterligare detaljer.

Därför är planen inte detsamma som en standardavtalsklausul. Ett alternativ är att behålla planen som en separat teknisk bilaga till avtalet, som kan ändras/uppdateras av parterna separat. Alternativt kanske parterna vill göra bilagan till en del av själva avtalet.

Denna bilaga kan vara en standardplan för byte och utträde som föreslås av leverantören och godkänns av kunden, eller en anpassad plan för byte och utträde som föreslås av leverantören för kunden.

Parterna kan uppdatera bytes och utträdesplanen under avtalets löptid i enlighet med utvecklingen av databehandlingstjänsterna och de data som omfattas av avtalet, vid tidpunkter som parterna kommer överens om. Denna uppdatering kan också påverka den överenskomna övergångsperioden, till exempel inom de gränser som fastställs i dataförordningen.

Bytes- och utträdesplanen gäller endast när kunden byter leverantör eller går över till en lokal IKT-infrastruktur, inte om kunden avser att radera sina data vid uppsägningstidens slut.

Alternativ B: Självbetjäningsverktyg för automatiserat byte

Även om självbetjäningsverktyg för automatiserat byte är vanliga kan de medföra vissa utmaningar. En särskild oro är till exempel att i fallet med SaaS kan vissa databaser och deras inställningar kanske inte migreras korrekt och/eller fullständigt, vilket medför att leverantören måste ingripa manuellt. Om leverantören förlitar sig på en sådan självbetjäningslösning, gör klausulerna i alternativ B det möjligt för kunden att säkerställa att avtalet innehåller tillräcklig information om processen och verktyget. De delar som ingår i alternativ A (bytes- och utträdesplan som bilaga till avtalet) kan tjäna som inspiration.

Om en leverantör använder bytesverktyg för att utföra de åtgärder som föreskrivs i dataförordningen för byte till en annan leverantörs system eller till lokal IKT-infrastruktur, skulle det anses utgöra en bytesavgift att debitera kunden för användningen av dessa bytesverktyg.

Vad händer om bytet misslyckas? Klausul 1.7 i alternativ A och klausul 2.6 i alternativ B behandlar situationer där bytet misslyckas genom att ange de åtgärder som kunden (och destinationsleverantören) och den ursprungliga leverantören måste vidta i god tro för att genomföra ett framgångsrikt byte och/eller utlösa den möjlighet till radering av data som dataförordningen ger.

Exempel: Den ursprungliga leverantören föreslår SaaS-lösning A och destinationsleverantören föreslår SaaS-lösning B. Kunden ber den ursprungliga leverantören att hjälpa till att byta till destinationsleverantören genom att exportera och överföra kundens exporterbara data till en specifik server. Följande situationer kan uppstå:

1. Den ursprungliga leverantören föreslår inte effektiva verktyg och förfaranden för att exportera och överföra alla exporterbara data till den specifika servern.
2. Data har levererats till den specifika servern, men kunden eller destinationsleverantören kan inte ladda upp data på rätt sätt.

1. Alternativ A: Byte och utträde med en plan som bilaga till avtalet

1.1. Information

1.1.1. Parterna bekräftar att leverantören i en bilaga till avtalet eller på sin webbplats har tillhandahållit kunden tydlig information om

(a) standardavgifter för tjänster och, i förekommande fall, straffavgifter för förtida uppsägning,

(b) bytesavgifter,

(c) tjänster som innebär mycket komplexa eller kostsamma byten, eller för vilka det är omöjligt att byta utan betydande störningar i data, digitala tillgångar eller tjänstearkitekturen, i förekommande fall,

(d) specifika tjänster där skyldigheterna vid byte och utträde inte gäller, i förekommande fall.

Artikel 31 i dataförordningen fastställer en särskild ordning för vissa databehandlingstjänster. För skräddarsydda eller mycket individualiserade tjänster gäller inte vissa skyldigheter vid byte. Parterna måste komma överens om hur ett sådant byte ska ske (inklusive kostnaden). För databehandlingstjänster som tillhandahålls som en icke-produktionsversion för testnings- och utvärderingsändamål och under en begränsad tidsperiod gäller inte skyldigheterna vid byte. Även om dessa standardavtalsklausuler inte har utformats för att täcka sådana situationer, kan de ändå tjäna som inspiration för parterna i ett avtal som rör sådana tjänster.

Enligt artikel 30.6 i dataförordningen är leverantörer inte skyldiga att utveckla ny teknik eller nya tjänster. De är inte heller skyldiga att lämna ut eller överföra digitala tillgångar till en kund eller en annan leverantör av databehandlingstjänster som i) skyddas av immateriella rättigheter, ii) utgör en företagshemlighet eller iii) äventyrar kundens eller leverantörens säkerhet och tjänstens integritet.

1.2. **Byte och utträde**

1.2.1. Parterna kommer överens om en ”bytes- och utträdesplan” (*planen*) med hjälp av det formulär som anges i tillägg 1, som utgör en integrerad del av avtalet och kommer att genomföras av parterna. Planen innehåller

(a) en uttömmande specifikation av alla kategorier av data och digitala tillgångar som kan överföras, inklusive minst alla exporterbara data (artikel 25.2 e i dataförordningen),

(b) en uttömmande specifikation av kategorier av data som är specifika för den interna funktionen av leverantörens databehandlingstjänst och som kommer att undantas från exporterbara data om det finns risk för överträdelse med avseende på leverantörens företagshemligheter (artikel 25.2 f i dataförordningen),

(c) tydlig information om kända risker för kontinuiteten i tillhandahållandet av funktioner eller tjänster från den ursprungliga leverantören av databehandlingstjänster (artikel 25.2 a iii i dataförordningen),

(d) detaljer om hjälp med byte och utträde, inklusive porteringsmetoder och format, samt de steg som krävs för att genomföra bytet,

(e) namn och kontaktuppgifter för den representant som kunden och leverantören har utsett för att genomföra planen,

(f) en uppskattning av den tid som behövs för att exportera och överföra data och digitala tillgångar från den ursprungliga leverantörens miljö.

Den ursprungliga leverantören kan stödja kundens byte genom att tillhandahålla en uppskattning av den tid som behövs för att exportera och transportera exporterbara data utanför sin miljö, baserat på den tid som krävs för att importera data, den uppskattade volymen, nätverkskapaciteten och tidigare erfarenheter eller tester. På samma sätt kan kunden uppskatta den tid som krävs för att importera och implementera data i destinationsmiljön. Båda parter bör utnyttja sådan information för att se om en alternativ övergångsperiod behövs.

(g) tekniska och andra begränsningar, inklusive sådana som uppstår vid lagring av data utanför Europeiska unionen,

(h) en beskrivning av den sekvens av byten som leverantören föreslår,

(i) en beskrivning av den testmetod som leverantören föreslår om tester genomförs.

1.2.2. Leverantören förser kunden med en hänvisning till det onlineregister med datastrukturer och dataformat, relevanta standarder och öppna interoperabilitetsspecifikationer där exporterbara data finns tillgängliga på [*ange länk till platsen*] (artikel 26 b i dataförordningen).

1.2.3. Om kunden så begär måste leverantören via lämpliga elektroniska medel tillhandahålla information som förklarar de relevanta förfarandena för kundens utsedda personal (eller auktoriserade tredje parter).

1.2.4. Om kunden så begär ska leverantören antingen ordna ett test eller hjälpa kunden att genomföra ett test, enligt överenskommelse i tillägg 1, för att kontrollera att planen fungerar i praktiken för exporterbara data och digitala tillgångar. Om problem uppstår under testet ska parterna i god tro analysera orsakerna och komma överens om lösningar.

1.2.5. Leverantören och kunden ska uppdatera planen när det är nödvändigt eller på kundens begäran, med en motivering för de nödvändiga ändringarna.

1.3. **Inledande av bytesprocessen**

1.3.1. Kunden inleder bytet genom att skicka ett meddelande om byte till leverantören enligt klausul 1.10, med iakttagande av uppsägningstiden på [*parterna anger den överenskomna uppsägningstiden, som inte får överstiga två månader*]. Om kunden endast vill byta vissa tjänster och motsvarande data eller digitala tillgångar, måste detta anges i meddelandet om byte. [ALTERNATIV] [Kunden meddelar detta genom att använda formuläret i **tillägg 3**].

I enlighet med villkoren i avtalet kan kunden välja att endast byta en viss delmängd av de tjänster som tillhandahålls av den ursprungliga leverantören. I så fall gäller skyldigheterna vid byte endast sådana tjänster och motsvarande data och digitala tillgångar; för övrigt gäller de tidigare överenskomna avtalsvillkoren fortfarande.

1.3.2. I meddelandet om byte informerar kunden leverantören om huruvida denne avser att

(a) byta till en annan leverantör av databehandlingstjänster. I detta fall tillhandahåller kunden nödvändiga uppgifter om destinationsleverantören (artikel 25.3 a i dataförordningen),

(b) byta till en lokal IKT-infrastruktur hos kunden (artikel 25.3 b i dataförordningen), eller

(c) inte byta leverantör utan endast radera sina exporterbara data och digitala tillgångar (artikel 25.3 c i dataförordningen).

(d) [ALTERNATIV] [Kunden meddelar detta genom att använda formuläret i **tillägg 4**].

1.3.3. Leverantören bekräftar mottagandet av meddelandet om byte till kunden senast [inom tre arbetsdagar] med hjälp av samma kommunikationsmedel som kunden använt.

1.4. **Övergångsperiod**

1.4.1. Kunden har rätt att byta leverantör utan oskäligt dröjsmål inom en övergångsperiod på högst 30 dagar. Kunden kan komma överens med leverantören om en övergångsperiod på (*parterna anger den överenskomna övergångsperioden, som kan vara högst 30 kalenderdagar*) (artikel 25.2 a i dataförordningen).

1.4.2. Om leverantören inte kan respektera den [obligatoriska maximala] övergångsperioden på grund av att detta inte är tekniskt genomförbart, ska leverantören (artikel 25.4 i dataförordningen)

(a) meddela kunden inom 14 arbetsdagar från [datumet för meddelandet om byte],

(b) ange en alternativ övergångsperiod, som inte får överstiga sju (7) månader från datumet för kundens meddelande om byte och

(c) ge en lämplig motivering till den tekniska ogenomförbarheten.

1.4.3. Kunden bekräftar mottagandet av meddelandet om en alternativ övergångsperiod [inom tre arbetsdagar].

1.4.4. Kunden kan förlänga övergångsperioden en gång, till en period som kunden anser vara mer lämplig för sina egna ändamål, dock inte längre än [*ange antal månader*] (artikel 25.5 i dataförordningen). I så fall meddelar kunden leverantören sin avsikt enligt överenskommelsen i klausul 1.11 före utgången av den ursprungliga övergångsperioden och anger den alternativa övergångsperioden. Leverantören bekräftar mottagandet av ett sådant meddelande om förlängning [inom tre arbetsdagar].

1.4.5. [ALTERNATIV] Kunden meddelar en alternativ övergångsperiod genom att använda formuläret i tillägg 5.

1.5. **Leverantörens skyldigheter under bytesprocessen**

1.5.1. Leverantören åtar sig att ge rimligt bistånd till kunden och tredje parter som bemyndigats av kunden i bytesprocessen när bytesprocessen inleds och under hela processen, så att kunden kan byta inom övergångsperioden. För detta ändamål måste leverantören särskilt

(a) tillhandahålla resurser, adekvat information (inklusive dokumentation som är nödvändig för att genomföra bytet) och tekniskt stöd; om problem upptäcks ska leverantören och kunden i god tro analysera orsakerna och komma överens om lösningar,

(b) iaktta vederbörlig omsorg för att upprätthålla driftskontinuitet och fortsätta att tillhandahålla funktioner eller tjänster enligt avtalet (artikel 25.2 a ii i dataförordningen),

(c) upprätthålla en hög säkerhetsnivå under hela bytesprocessen, särskilt för säkerheten för data under överföringen (artikel 25.2 a iv i dataförordningen).

1.6. **Kundens skyldigheter under bytesprocessen**

1.6.1. Kunden åtar sig att vidta alla rimliga åtgärder för att uppnå ett effektivt byte. Kunden ansvarar för att importera data och digitala tillgångar till sina egna system eller till destinationsleverantörens system och implementera dessa data och digitala tillgångar i dessa system, även om kunden använder en tredje parts tjänster för dessa åtgärder.

1.6.2. Om tillämpligt och utan att det påverkar artikel 30.6 i dataförordningen, åtar sig kunden och leverantören, eller tredje part som kunden har bemyndigat, att respektera immateriella rättigheter till allt material som tillhandahålls av leverantören under bytesprocessen, samt leverantörens företagshemligheter. Kunden åtar sig att ge åtkomst till och möjliggöra användning av detta material för tredje part som de har bemyndigat endast i den utsträckning som är nödvändig för att slutföra bytet och endast efter leverantörens uttryckliga tillstånd. Åtkomsten till och användningen av leverantörens material som är relaterat till bytet och som skyddats av immateriella rättigheter och/eller företagshemligheter relaterade till bytet ska upphöra senast vid utgången av den överenskomna övergångsperioden, inklusive den alternativa övergångsperioden, i full överensstämmelse med de sekretessåtaganden och immateriella rättigheter som beviljats av leverantören.

1.6.3. Kunden agerar i god tro för att genomföra alla riktlinjer relaterade till bytet som delas av leverantören.

1.6.4. Kunden kan komma överens om mått på ett framgångsrikt byte samt delmål för bytet med den ursprungliga leverantören och informerar den ursprungliga leverantören om i vilken utsträckning dessa delmål har uppnåtts under bytet. I alla händelser ska kunden informera leverantören om att bytet har slutförts framgångsrikt.

Utöver skyldigheterna i detta avtal har alla berörda parter, inklusive destinationsleverantörer av databehandlingstjänster, en lagstadgad skyldighet enligt artikel 27 i dataförordningen att samarbeta i god tro för att göra bytesprocessen effektiv, möjliggöra en snabb överföring av data och upprätthålla kontinuiteten i databehandlingstjänsterna.

1.7. **Misslyckat byte**

1.7.1. Om bytet inte slutförs framgångsrikt måste parterna samarbeta i god tro för att identifiera orsaken och slutföra bytet, möjliggöra en snabb överföring av data och upprätthålla kontinuiteten i tjänsterna. På kundens begäran ska leverantören särskilt stödja kunden i att identifiera orsakerna till att bytet inte lyckades och, i den mån de identifierade orsakerna är relaterade till leverantörens miljö eller bytesprocesser, ge råd om hur de identifierade tekniska problemen kan lösas. De regler som gäller för bytesavgifter gäller för det stöd som leverantören tillhandahåller och andra tjänster från leverantören som avses i detta avsnitt.

1.7.2. Kunden kan bemyndiga destinationsleverantören att agera på kundens vägnar.

1.8. **Hämtning och radering av data**

1.8.1. Kunden kan hämta eller radera sina data under den överenskomna perioden för hämtning av data, som är […] dagar.

1.8.2. Vid slutet av den överenskomna perioden för hämtning av data, och om bytet har slutförts framgångsrikt, raderar leverantören alla exporterbara data och digitala tillgångar som genererats av kunden eller som är direkt relaterade till kunden. Leverantören bekräftar [inom x arbetsdagar] att sådan radering har slutförts, med undantag för exporterbara personuppgifter som leverantören är skyldig att lagra enligt unionsrätt eller nationell rätt.

Hämtning av data påbörjas efter det att den överenskomna övergångsperioden har löpt ut och måste ske minst 30 kalenderdagar efter utgången av den övergångsperiod som överenskommits mellan kunden och leverantören. Kunden kan besluta att inte utnyttja sin rätt att hämta data. I sådant fall kommer antingen kunden att radera data på egen hand (och kan informera leverantören om detta enligt artikel 25.3 c i dataförordningen), eller så kommer leverantören att radera sådana icke-hämtade data enligt klausulerna 1.8.2 i alternativ A och 2.7.2 i alternativ B.

1.9. **Bytesavgifter**

1.9.1. De avgifter som kunden ska betala för bytet är följande […]

Vid parallell användning av flera databehandlingstjänster (multimolnscenario) betraktas avgifterna för datauttag inte som bytesavgifter och kan därför åläggas kunden i syfte att vidareföra sådana kostnader som leverantören ådragit sig, utan att överskrida de faktiska kostnaderna. I alla andra fall får inga bytesavgifter åläggas kunden efter den 12 januari 2027 (se förklaringarna om bytesavgifter i inledningen till dessa standardavtalsklausuler).

1.10. **Avslutande av bytesprocessen**

[Se standardavtalsklausulerna om uppsägning]

1.11. **Meddelanden**

Parterna är överens om att alla meddelanden mellan dem avseende byte och utträde ska ske [*parterna fyller i valt kommunikationsmedel, inklusive lämpliga elektroniska medel*].

1.12. **Prioritetsordning**

I händelse av konflikt eller inkonsekvens mellan dessa klausuler om byte och utträde och andra tillämpliga avtalsvillkor, bestämmelser eller andra tillämpliga avtal relaterade till byte mellan databehandlingstjänster, ska dessa klausuler ha företräde.

2. **Alternativ B: Byte och utträde med självbetjäningsverktyg för automatiserat byte**

2.1. **Information**

2.1.1. Innan leverantören tar emot beställningen av databehandlingstjänsterna har leverantören gett kunden tydlig information om

(a) tillgängliga självbetjäningsverktyg för automatiserat byte för sådana tjänster (*bytesverktyg*) och villkoren för deras användning,

(b) standardavgifter för tjänster och, i förekommande fall, straffavgifter för förtida uppsägning,

(c) bytesavgifterna, inklusive avgifterna för användning av bytesverktygen.

Artikel 31 i dataförordningen fastställer en särskild ordning för vissa databehandlingstjänster. För skräddarsydda eller mycket individualiserade tjänster gäller vissa skyldigheter vid byte inte. Parterna måste komma överens om hur ett sådant byte ska ske (inklusive kostnaden). För databehandlingstjänster som tillhandahålls som en icke-produktionsversion för testnings- och utvärderingsändamål och under en begränsad tidsperiod gäller inte skyldigheterna vid byte. Även om dessa standardavtalsklausuler inte har utformats för att täcka sådana situationer, kan de ändå tjäna som inspiration för parterna i ett avtal som rör sådana tjänster.

Enligt artikel 30.6 i dataförordningen är leverantörer inte skyldiga att utveckla ny teknik eller nya tjänster. De är inte heller skyldiga att till en kund eller en annan leverantör av databehandlingstjänster lämna ut eller överföra digitala tillgångar som i) skyddas av immateriella rättigheter, ii) utgör en företagshemlighet eller iii) äventyrar kundens eller leverantörens säkerhet och tjänstens integritet.

2.1.2. Checklistan för byte i **tillägg 2**, som utgör en integrerad del av avtalet, innehåller

(a) en uttömmande specifikation av alla kategorier av data och digitala tillgångar som kan överföras med hjälp av bytesverktyg, inklusive minst alla exporterbara data (artikel 25.2 e i dataförordningen),

(b) en uttömmande specifikation av kategorier av data som är specifika för den interna funktionen av leverantörens databehandlingstjänst och som kommer att undantas från exporterbara data om det finns risk för överträdelse med avseende på leverantörens företagshemligheter (artikel 25.2 f i dataförordningen),

(c) information om förfaranden för byte och portering med hjälp av bytesverktyg, inklusive metoder och format, tekniska och andra begränsningar (inklusive sådana som uppstår till följd av lagring av data utanför EU), förfaranden, dokumentation samt, i tillämpliga fall, bästa praxis, kapacitet och tekniskt stöd som leverantören kommer att ställa till kundens förfogande (särskilt under testning, förberedelse inför byte och själva bytet), inklusive eventuella hjälplinjer som är tillgängliga för kunderna under bytet eller alternativa kommunikationskanaler och testscenarier. Denna information måste förklara hur man byter alla exporterbara data och digitala tillgångar på ett sammanhängande och konsekvent sätt tillräckligt snabbt för att bytet ska bli effektivt,

(d) en uppskattning av den tid som behövs för att exportera och överföra data och digitala tillgångar från den ursprungliga leverantörens miljö, när bytesverktygen används i enlighet med leverantörens dokumentation,

(e) tydlig information om kända risker för kontinuiteten i tillhandahållandet av funktioner eller tjänster från den ursprungliga leverantören av databehandlingstjänster (artikel 25.2 a iii i dataförordningen),

(f) de resurser, inklusive it-resurser (såsom servrar, centralprocessor, minne, I/O, bandbredd), som leverantören kommer att tillhandahålla för att säkerställa ett effektivt byte och förfarandet för att erhålla ytterligare it-resurser.

2.1.3. Leverantören förser kunden med en hänvisning till det onlineregister med datastrukturer och dataformat, relevanta standarder och öppna interoperabilitetsspecifikationer där exporterbara data finns tillgängliga på [*ange länk till platsen*] (artikel 26 b i dataförordningen).

2.2. **Inledande av bytesprocessen**

2.2.1. Kunden inleder bytet genom att skicka ett meddelande om byte till leverantören enligt klausul 2.10, med iakttagande av uppsägningstiden på [*parterna anger den överenskomna uppsägningstiden, som inte får överstiga två månader*]. Om kunden endast vill byta vissa tjänster och motsvarande data eller digitala tillgångar, måste detta anges i meddelandet om byte. [ALTERNATIV] [Kunden meddelar detta genom att använda formuläret i **tillägg 3**].

Meddelandet om byte är ett annat instrument än ett meddelande om avtalets upphörande. I enlighet med villkoren i avtalet kan kunden välja att endast byta en viss delmängd av de tjänster som tillhandahålls av den ursprungliga leverantören. I så fall gäller skyldigheterna vid byte endast sådana tjänster och motsvarande data och digitala tillgångar; för övrigt gäller de tidigare överenskomna avtalsvillkoren fortfarande.

2.2.2. I meddelandet om byte informerar kunden leverantören om huruvida denne avser att

(a) byta till en annan leverantör av databehandlingstjänster; i detta fall ska kunden tillhandahålla nödvändiga uppgifter om destinationsleverantören,

(b) byta till en lokal IKT-infrastruktur hos kunden, eller

(c) inte byta utan endast radera sina exporterbara data och digitala tillgångar.

(d) [ALTERNATIV] [Kunden meddelar detta genom att använda formuläret i **tillägg 4**].

2.2.3. Kunden kan också i meddelandet om byte ange tidsfönstret/tidsfönstren för bytet och de ytterligare it-resurser som kunden behöver under dessa tidsfönster. Om leverantören inte kan säkerställa sådana it-resurser under de angivna tidsfönstren, ska denne invända senast [tre arbetsdagar] efter mottagandet av meddelandet om byte, med vederbörlig motivering, och föreslå flera alternativa ”tidsfönster” för kunden, med beaktande av den maximala övergångsperioden.

Tidsfönstret/tidsfönstren för bytet är en period, till exempel en helg, under vilken kunden avser att göra sina system otillgängliga för användarna och ingen uppdatering sker så att data fryses och kunden kan genomföra bytet.

2.2.4. Leverantören bekräftar mottagandet av meddelandet om byte till kunden [inom tre arbetsdagar] med hjälp av samma kommunikationsmedel som kunden använt.

Kunden kan behöva genomföra bytet inom en viss tidsram för att minimera störningar i verksamheten. Dessutom kan bytet kräva ytterligare resurser från den ursprungliga leverantören. Därför bör kunden, om det behövs, ange de tidsfönster under vilka denne avser att genomföra bytet och ytterligare resurser (i enlighet med information från den ursprungliga leverantören). Om den ursprungliga leverantören av berättigade skäl inte kan tillhandahålla sådana resurser inom dessa tidsfönster (t.ex. planerat underhåll av tjänster som allvarligt skulle påverka resursernas tillgänglighet under den tiden), bör denne tillhandahålla kunden alternativ som säkerställer ett effektivt byte före utgången av den maximala övergångsperioden.

2.3. **Övergångsperiod**

2.3.1. Om leverantören inte kan respektera den [obligatoriska maximala] övergångsperioden på grund av att detta inte är tekniskt genomförbart, ska leverantören

(a) skriftligen, inklusive via lämpliga elektroniska medel, underrätta kunden inom 14 arbetsdagar från [datumet för meddelandet om byte],

(b) ange en alternativ övergångsperiod, som inte får överstiga sju (7) månader från datumet för kundens meddelande om byte, och

(c) ge en lämplig motivering till den tekniska ogenomförbarheten.

Kunden bekräftar mottagandet av ett sådant meddelande om förlängning [inom tre arbetsdagar].

2.3.2. Kunden kan förlänga övergångsperioden en gång, till en period som kunden anser vara mer lämplig för sina egna ändamål, dock inte längre än [*ange antal månader*]. I så fall meddelar kunden leverantören skriftligen, inklusive via lämpliga elektroniska medel, sin avsikt före utgången av den ursprungliga övergångsperioden och anger den alternativa övergångsperioden. Leverantören bekräftar mottagandet av ett sådant meddelande om förlängning [inom tre arbetsdagar].

[ALTERNATIV] [Kunden meddelar detta genom att använda formuläret i **tillägg 5**].

2.4. Leverantörens skyldigheter under bytesprocessen

2.4.1. Leverantören åtar sig att ge rimligt bistånd till kunden och tredje parter som bemyndigats av kunden i bytesprocessen när bytesprocessen inleds och under hela processen, så att kunden kan byta inom övergångsperioden. För detta ändamål måste leverantören särskilt

(a) iaktta vederbörlig omsorg för att upprätthålla driftskontinuitet och fortsätta att tillhandahålla funktioner eller tjänster enligt avtalet,

(b) upprätthålla en hög säkerhetsnivå under hela bytesprocessen, särskilt för säkerheten för data under överföringen, och

(c) om problem upptäcks under bytet och inte kan lösas genom tekniskt stöd, tillsammans med kunden analysera orsakerna och komma överens om lösningar.

Även i alternativ B ”Självbetjäningsverktyg för automatiserat byte” delar leverantören ansvaret för tidpunkten för bytet, till exempel om verktygen är för långsamma för att säkerställa ett framgångsrikt byte eller om leverantören reagerar med oskäligt dröjsmål när kunden upptäcker ett problem som kräver leverantörens hjälp.

2.5. Kundens skyldigheter under bytesprocessen

2.5.1. Kunden åtar sig att vidta alla rimliga åtgärder för att uppnå ett effektivt byte. Kunden ansvarar för att importera data och digitala tillgångar till sina egna system eller till destinationsleverantörens system och implementera dessa data och digitala tillgångar, även om kunden använder en tredje parts tjänster för dessa åtgärder.

2.5.2. Om tillämpligt och utan att det påverkar artikel 30.6 i dataförordningen, åtar sig kunden och leverantören, eller tredje part som kunden har bemyndigat, att respektera immateriella rättigheter till allt material som tillhandahålls av leverantören under bytesprocessen, samt leverantörens företagshemligheter. Kunden åtar sig att ge åtkomst till och möjliggöra användning av detta material för tredje part som de har bemyndigat endast i den utsträckning som är nödvändig för att slutföra bytet och endast efter leverantörens uttryckliga tillstånd. Åtkomsten till och användningen av leverantörens material som är relaterat till bytet och som skyddats av immateriella rättigheter och/eller företagshemligheter relaterade till bytet ska upphöra senast vid utgången av den överenskomna övergångsperioden, inklusive den alternativa övergångsperioden, i full överensstämmelse med de sekretessåtaganden och immateriella rättigheter som beviljats av leverantören.

2.5.3. Kunden kan komma överens om mått på ett framgångsrikt byte samt delmål för bytet med den ursprungliga leverantören och informerar den ursprungliga leverantören om i vilken utsträckning dessa delmål har uppnåtts under bytet. I alla händelser ska kunden informera leverantören om att bytet har slutförts framgångsrikt.

2.5.4. Kunden agerar i god tro för att genomföra alla riktlinjer relaterade till bytet som delas av leverantören.

Utöver skyldigheterna i detta avtal har alla berörda parter, inklusive destinationsleverantörer av databehandlingstjänster, en lagstadgad skyldighet enligt artikel 27 i dataförordningen att samarbeta i god tro för att göra bytesprocessen effektiv, möjliggöra en snabb överföring av data och upprätthålla kontinuiteten i databehandlingstjänsterna.

De rimliga åtgärder som kunden ska vidta för att uppnå ett effektivt byte omfattar särskilt följande:

— Förbereda bytet internt (t.ex. blockera all åtkomst till data och informera användaren om att systemet inte är tillgängligt; om en tredje part anlitas för bytet, ge denna tredje part lämpliga instruktioner så att den respekterar avtalet mellan kunden och leverantören).

— Övervaka bytet (t.ex. kontrollera exporterade data och digitala tillgångar under bytet för att omedelbart identifiera eventuella problem).

— Utarbeta lämpliga avtalsvillkor med destinationsleverantören eller säkerställa lämpliga resurser för byte på plats.

2.6. **Misslyckat byte**

2.6.1. Om bytet inte slutförs framgångsrikt måste parterna samarbeta i god tro för att identifiera orsaken och slutföra bytet, möjliggöra en snabb överföring av data och upprätthålla kontinuiteten i tjänsterna. På kundens begäran ska leverantören särskilt stödja kunden i att identifiera orsakerna till att bytet inte lyckades och, i den mån de identifierade orsakerna är relaterade till leverantörens miljö eller bytesprocesser, ge råd om hur de identifierade tekniska problemen kan lösas. De regler som gäller för bytesavgifter gäller för det stöd som leverantören tillhandahåller och andra tjänster från leverantören som avses i detta avsnitt.

2.6.2. Kunden kan bemyndiga destinationsleverantören att agera på kundens vägnar.

2.7. **Hämtning och radering av data**

2.7.1. Parterna är överens om att kunden hämtar eller raderar sina data under den överenskomna perioden för hämtning av data, som är […] dagar.

2.7.2. Vid slutet av den överenskomna perioden för datahämtning, och om bytet har slutförts framgångsrikt, åtar sig leverantören att radera alla exporterbara data och digitala tillgångar som genererats av kunden eller som är direkt relaterade till kunden och bekräfta för kunden att så har skett, med undantag för exporterbara data som leverantören är skyldig att lagra enligt obligatoriska EU-lagar eller lagar i EU:s medlemsstater, så länge leverantören meddelar kunden, om lagen tillåter det, vilka exporterbara data som kommer att behållas, hur länge och på vilka grunder.

Hämtning av data påbörjas efter det att den överenskomna övergångsperioden har löpt ut och måste ske minst 30 kalenderdagar efter utgången av den övergångsperiod som överenskommits mellan kunden och leverantören. Kunden kan besluta att inte utnyttja sin rätt att hämta data. I sådant fall kommer antingen kunden att radera data på egen hand (och kan informera leverantören om detta enligt artikel 25.3 c i dataförordningen), eller så kommer leverantören att radera sådana icke-hämtade data enligt klausulerna 1.8 i alternativ A och 2.7 i alternativ B.

2.8. **Bytesavgifter**

De avgifter som kunden ska betala för bytet är följande […]

Vid parallell användning av flera databehandlingstjänster (multimolnscenario) betraktas avgifterna för datauttag inte som bytesavgifter och kan därför åläggas kunden i syfte att vidareföra sådana kostnader som leverantören ådragit sig, utan att överskrida de faktiska kostnaderna. Testverktygen för byte och leverantörens rimliga stöd till kunden vid testning enligt överenskommelse i planen ska betraktas som en del av bytesprocessen, och följaktligen ska avgifterna för sådana tjänster gradvis avskaffas i enlighet med artikel 29 i dataförordningen.

2.9. **Avslutande av bytesprocessen**

Se klausul 1 i standardavtalsklausulerna om uppsägning.

2.10. **Meddelanden**

Parterna är överens om att alla meddelanden mellan dem avseende byte och utträde ska ske [*parterna fyller i valt kommunikationsmedel, inklusive lämpliga elektroniska medel*].

2.11. **Prioritetsordning**

I händelse av konflikt eller inkonsekvens mellan dessa klausuler om byte och utträde och andra tillämpliga avtalsvillkor, bestämmelser eller andra tillämpliga avtal relaterade till byte mellan databehandlingstjänster, ska dessa klausuler ha företräde.

Tillägg 1

Bytes- och utträdesplan

1. **Kontaktuppgifter**

(a) Leverantörens kontaktperson för byte och utträde: …

(b) Kundens kontaktperson för byte och utträde: …

2. **Kunden måste ange följande information i det skriftliga meddelandet:**

(a) Data som berörs av meddelandet, enligt den överenskomna identifieringen i **tillägg 2**.

(b) Destination för data: Kundens lokala IKT-infrastruktur eller en destinationsleverantör, inklusive relevanta tekniska specifikationer om destinationsplatsen.

(c) Plats där data ska exporteras och transporteras.

3. **Leverantörens skyldigheter att reagera på det skriftliga meddelandet**

Inom … dagar ska leverantören svara kunden skriftligen med följande information:

(a) En uttömmande specifikation av alla kategorier av data som ska överföras under bytet

i) Exporterbara data

— Alla data som importerats av kunden vid tjänsteavtalets början, inklusive metadata (*inmatade data*)

— A, med metadata: … i format …

— B, med metadata: … i format …

— C, med metadata: … i format …

— Alla data som direkt eller indirekt genererats genom kundens användning av databehandlingstjänsten:

— D, med metadata: … i format …

— E, med metadata: … i format …

— F, med metadata: … i format …

ii) Digitala tillgångar:

— L, i format …

— M, i format …

(b) En uttömmande specifikation av kategorier av data som är specifika för den interna funktionen av leverantörens databehandlingstjänst och som ska undantas från exporterbara data om det finns risk för överträdelse med avseende på leverantörens företagshemligheter: …

4. **Bekräftelse av data som ska bytas**

Kunden anger vilka data och digitala tillgångar som ska överföras inom den överenskomna (eller alternativa) övergångsperioden.

5. **Ordning, tidpunkt och testning**

Under övergångsperioden

(a) är den överenskomna ordningen och tidpunkten för export och överföring av de valda uppgifterna och digitala tillgångarna följande: …

(b) är beskrivningen av den testmetod som leverantören föreslår: ....

(c) kommer leverantören eller kunden med hjälp av leverantörens verktyg och processer att testa exporten och överföringen till den överenskomna platsen med en del av överenskomna data och digitala tillgångar, för att bekräfta eller anpassa ordningen och tidpunkten,

(d) kommer kunden att testa importen till och implementeringen av överenskomna data och digitala tillgångar i sina egna system eller i destinationsleverantörens system,

(e) om det uppstår problem med testningen eller testresultaten, kommer den ursprungliga leverantören och kunden att avgöra om dessa beror på exporten av överenskomna data och digitala tillgångar och överföringsprocesser som ligger under leverantörens ansvar eller på import- och implementeringsprocesser som ligger under kundens ansvar.

6. **Genomförande av bytesprocessen**

(a) Leverantören måste exportera och transportera data eller digitala tillgångar elektroniskt eller fysiskt till den plats som anges av kunden, och kunden (eller tredje part som kunden har bemyndigat) måste importera data eller digitala tillgångar till sina egna system eller till destinationsleverantörens system och implementera dessa data eller digitala tillgångar i dessa system.

(b) Kunden (eller tredje part som kunden har bemyndigat) måste testa funktionerna i sin miljö eller destinationsleverantörens miljö inom .... *[parterna anger den överenskomna tidsperioden för genomförandet av testet]* och dokumentera för leverantören eventuella problem som uppstår på grund av i) kvaliteten på data eller digitala tillgångar som exporterats eller ii) otillräcklig information från leverantören.

(c) Leverantören måste reagera utan oskäligt dröjsmål så att kunden kan byta inom den obligatoriska övergångsperioden.

7. **Framgångsrikt byte**

Så snart kunden meddelar leverantören att bytet har slutförts, åtar sig leverantören att utan oskäligt dröjsmål meddela kunden om att avtalet har upphört. Om kunden inte meddelar leverantören om att bytet har genomförts eller inte, medan leverantören har skäl att tro att bytet har slutförts framgångsrikt av kunden, kan leverantören skicka en begäran till kunden om bekräftelse på att bytet har slutförts framgångsrikt. Om kunden inte bekräftar att bytet har slutförts framgångsrikt inom 30 kalenderdagar från sådan begäran, anses bytet inte ha slutförts framgångsrikt och avtalet kommer inte att upphöra.

Tillägg 2

Checklista för byte

Antingen anges den erforderliga informationen uttryckligen nedan, eller så finns den erforderliga informationen på […]

(a) En uttömmande specifikation av alla kategorier av data och digitala tillgångar som kan överföras, inklusive minst alla exporterbara data: …

(b) En uttömmande specifikation av kategorier av data och digitala tillgångar som är specifika för den interna funktionen av leverantörens databehandlingstjänst, med risk för överträdelse med avseende på leverantörens företagshemligheter, som är undantagna från byte: …

(c) Information om förfaranden för byte och portering med hjälp av bytesverktyg: …

(d) Uppskattning av den tid som behövs för att exportera och överföra data och digitala tillgångar: …

(e) Kända risker för kontinuiteten i tillhandahållandet av den ursprungliga leverantörens funktioner eller tjänster: …

(f) It-resurser som leverantören kommer att säkerställa för ett effektivt byte: …

Tillägg 3

Meddelande om byte

[Leverantörens namn och adress för kommunikation]

[Datum]

Meddelande om byte

Kundens namn: […]

Avtal: (*namn och uppgifter om avtalet, t.ex. avtalets namn, nummer, datum för ingående, enligt avtalets krav*)

Tjänster som byts: [*alla som omfattas av avtalet*] eller [*ange uttryckligen tjänster eller digitala tillgångar som omfattas av bytet om endast en del av tjänsterna ska omfattas av bytet*]

[ALTERNATIV] [På kundens vägnar meddelar jag/vi att kunden inleder bytet av de tjänster som omfattas av bytet från och med (*ange startdatum*). Uppsägningstiden är (*anges av kunden: högst två månader, kan vara kortare efter kundens gottfinnande*].

[ALTERNATIV] [På kundens vägnar meddelar jag/vi att kunden inleder bytet av följande tjänster, data eller digitala tillgångar: …

[ALTERNATIV] Kunden informerar er om sin avsikt att byta till [*uppgifter om ny leverantör/kundens lokala infrastruktur*].

[ALTERNATIV] [*(Tillämpligt för automatiserat byte)* Kunden önskar byta inom följande tidsfönster: (*ange datum och uppgifter*). Kunden begär att följande it-resurser ska vara tillgängliga under dessa tidsfönster (*fylls i av kunden*)].

Kontaktuppgifter för den person som ansvarar för bytet: (*uppgifter om kundens representant som ansvarar för bytet*).

_____

[underskrift av kundens behöriga representant]

Tillägg 4

Meddelande om utträde

Detta formulär är tillämpligt om kunden inte vill byta leverantör utan endast radera sina exporterbara data eller digitala tillgångar enligt både alternativ A och alternativ B.

[Leverantörens namn och adress för kommunikation]

[Datum]

Meddelande om utträde

Kundens namn: […]

Avtal: [*namn och uppgifter om avtalet, t.ex. avtalets namn, nummer, datum för ingående, enligt avtalets krav*]

Raderade data/digitala tillgångar: [(*allt som omfattas av avtalet*] eller [*ange uttryckligen vilka data eller digitala tillgångar som ska raderas*]

[ALTERNATIV] [På kundens vägnar meddelar jag/vi att kunden inleder ett byte som endast består av radering av raderade data/digitala tillgångar från och med (*startdatum*). Uppsägningstiden är (*anges av kunden: högst två månader, kan vara kortare efter kundens gottfinnande*)].

[ALTERNATIV] [Kontaktuppgifter för den person som ansvarar för bytet: (*uppgifter om kundens representant som ansvarar för bytet*)].

_____

[underskrift av kundens behöriga representant]

Tillägg 5

Meddelande om alternativ övergångsperiod

[Leverantörens namn och adress för kommunikation]

[Datum]

Meddelande om alternativ övergångsperiod

Kundens namn: […]

Avtal: [*namn och uppgifter om avtalet, t.ex. avtalets namn, nummer, datum för ingående, enligt avtalets krav*]

Raderade data/digitala tillgångar: [*allt som omfattas av avtalet*] eller [*ange uttryckligen vilka data eller digitala tillgångar som ska raderas*]

[ALTERNATIV] [På kundens vägnar meddelar jag/vi att kunden önskar förlänga övergångsperioden till senast (*datum*)].

[ALTERNATIV] [Kontaktuppgifter för den person som ansvarar för bytet: (*uppgifter om kundens representant som ansvarar för bytet*).]

_____

[underskrift av kundens bemyndigade representant]

BILAGA VII

STANDARDAVTALSKLAUSULER

om uppsägning

Förordning (EU) 2023/2854 (nedan kallad *dataförordningen*) gör det möjligt för kunder till databehandlingstjänster (dvs. molntjänster och edgetjänster) att byta mellan leverantörer eller överföra sina data till sin egen lokala IKT-infrastruktur. Byte av leverantör påverkar huruvida avtalet mellan parterna ska fortsätta att gälla eller upphöra.

Dessa standardavtalsklausuler behandlar uppsägning av avtalet mellan kunden och leverantören avseende en viss tjänst i samband med byte av leverantör. Dessa standardavtalsklausuler omfattar processen för uppsägning av tjänsteavtalet. De är direkt kopplade till standardavtalsklausulerna om byte och utträde och innehåller olika uppsägningsmöjligheter och tillhörande villkor. Databehandlingsavtalet upphör vanligtvis (helt eller delvis) när bytet har slutförts eller om kunden inte vill byta till en annan leverantör utan begär att alla data ska raderas och sådan radering har genomförts. Dessa standardavtalsklausuler innehåller några ytterligare alternativ för att hjälpa parterna i situationer som inte omfattas av dataförordningen.

Avtalet med leverantören kan omfatta flera tjänster. Om dessa standardavtalsklausuler läggs till i avtalet och kunden sedan byter en tjänst till en destinationsleverantör medan de andra tjänsterna förblir hos den ursprungliga leverantören, upphör avtalet endast att gälla för denna specifika tjänst, om inte parterna kommer överens om något annat.

Utöver uppsägningen i samband med byte som omfattas av dessa standardavtalsklausuler kan avtalet också sägas upp på andra grunder för uppsägning som ingår i huvudavtalet eller som föreskrivs i tillämplig lag. Leverantören kan besluta att säga upp avtalet om kunden bryter mot sina skyldigheter och lämna in ett uppsägningsmeddelande. I detta fall kan kunden lämna in ett meddelande om byte, vilket innebär att avtalet förlängs till dess att bytet har genomförts.

Andra standardavtalsklausuler som rekommenderas av kommissionen finns bifogade och täcker andra specifika ämnen än uppsägning av avtalet. Parterna uppmuntras att överväga att använda även dessa andra klausuler, eftersom de har utformats för att vara samstämmiga och förstärka varandra.

Vad ingår i standardavtalsklausulerna om uppsägning?

Scenarier som anges i dataförordningen: Avtalet kommer att upphöra under särskilda omständigheter när bytet har slutförts framgångsrikt (*händelse A*) eller om kunden inte vill byta men kräver att alla data raderas och sådan radering har slutförts framgångsrikt (*händelse B*). Avtalet kommer att anses ha upphört när bytet har slutförts framgångsrikt (*händelse A*) eller vid utgången av den maximala uppsägningstiden (*händelse B*). Det finns inget behov av att delge uppsägningsmeddelandet eller följa uppsägningsförfarandet enligt avtalet, eftersom avtalet upphör automatiskt. Leverantören är dock skyldig att meddela kunden att avtalet anses ha upphört (artikel 25.2 c i dataförordningen). Detta meddelande är av informativ karaktär, eftersom avtalet redan har upphört. Även om leverantören försenar meddelandet kan denne därför inte ta ut någon avgift enligt det avslutade avtalet.

Kunden bör dock informera leverantören om att bytet har genomförts, eftersom leverantören kanske inte är medveten om detta. Om leverantören har skäl att tro att kunden redan har bytt leverantör (t.ex. om kunden inte loggar in på tjänsten eller inte har några data lagrade i tjänsten) kan leverantören kontakta kunden och begära bekräftelse på att bytet har genomförts. Om kunden inte svarar anses bytet inte ha slutförts framgångsrikt och avtalet fortsätter (dvs. det upphör inte) enligt befintliga villkor.

Dataförordningen definierar inte vad som avses med ett framgångsrikt byte. I princip åligger det kunden att avgöra om bytet har slutförts framgångsrikt. Kunden, eller kunden och leverantören, kan dock komma överens om att fastställa vissa kriterier för att bedöma om bytet har slutförts framgångsrikt, i synnerhet

(a) slutförande av dataöverföringen, dvs. om alla exporterbara data och, i förekommande fall, digitala tillgångar har överförts till destinationsleverantörens miljö, samt om deras noggrannhet, integritet och fullständighet har bibehållits; exporterbara data och digitala tillgångar ska överensstämma med ursprungliga data och digitala tillgångar utan förlust eller skada,

(b) användning av digitala tillgångar (om tillämpligt); om bytet innefattade överföring av digitala tillgångar, såsom kundens egna eller licensierade applikationer, bör kunden kontrollera om sådana digitala tillgångar är installerade, konfigurerade och körs i destinationsleverantörens miljö,

(c) testning av ny tjänst: i denna fas bör kunden kontrollera om de tjänster som erbjuds av destinationsleverantören fungerar som planerat före bytet; i synnerhet bör kunden testa prestanda, funktionalitet och drift av destinationsleverantörens tjänst, inklusive överförda data eller digitala tillgångar, för att bedöma om kriterierna för kontroll av bytet är uppfyllda.

Vid ett tidsbegränsat avtal kan bytet avslutas före avtalets utgång eller efter det (för det senare, se händelse D). Om bytet avslutas före avtalets utgång upphör även avtalet att gälla. I så fall kan straffavgifter för förtida uppsägning bli aktuella (artiklarna 23 a, 25.2 c och 29.4 i dataförordningen).

Vad händer om bytet misslyckas?

Se standardavtalsklausulerna om byte och utträde.

För att lösa en situation där bytet misslyckas och avtalet inte kan sägas upp kan parterna lämna in ett klagomål till den behöriga myndigheten enligt dataförordningen, så att myndigheten fattar ett beslut. Det bör dock klargöras att parterna också kan använda alla rättsliga medel som finns tillgängliga inom deras jurisdiktion (t.ex. lämna in en fordran, begära föreläggande från civila domstolar osv.).

Ytterligare två scenarier: Klausulerna 1.4 och 1.5 är valfria och presenterar ytterligare två scenarier som parterna kan överväga. Även om dessa inte uttryckligen nämns i dataförordningen kan de förekomma i praktiken och ingår i klausulerna för att hjälpa parterna att lösa sådana situationer. Dessa scenarier är följande:

— Kunden vill förlänga tillgängligheten av sina data från den ursprungliga leverantören eller upprätthålla avtalet med den ursprungliga leverantören genom att utnyttja alternativet att köpa en ny tjänst för en längre period, oavsett om detta föregås av ett byte av tjänst eller en enkel avslutning av tjänsten utan något byte. Kunden kan behöva en tjänst med begränsad funktionalitet från den ursprungliga leverantören, dvs. säkerställa tillgängligheten av sina data under denna längre period eller ha ett avtal som gör det möjligt att beställa den nya tjänsten (*händelse C*).

I detta fall, eftersom data kommer att vara tillgängliga genom en tjänst med begränsad funktionalitet, bör den ursprungliga leverantören och kunden ingå ett nytt avtal för denna ytterligare tjänst eller ändra det befintliga avtalet (se klausul 1.4.2). I synnerhet bör parterna komma överens om en ny period för datahämtning. När det gäller allmänna (ram)avtal kanske kunden vill behålla avtalsförhållandet med den ursprungliga leverantören för att snabbt kunna köpa nya tjänster utan att behöva genomgå processen med att ingå ett nytt avtal, vilket i större organisationer kan vara en långdragen och komplicerad process.

Exempel på händelse C: Kunden har exporterat och överfört sina data från den ursprungliga leverantören till destinationsleverantören, i vars miljö data har implementerats framgångsrikt. Ett annat exempel kan vara att kunden beslutar att avsluta tjänsten hos den ursprungliga leverantören utan att därefter migrera till en annan leverantör. I båda exemplen vill kunden dock inte att kundens data ska raderas, utan föredrar att de säkerhetskopieras hos den ursprungliga leverantören även efter den överenskomna perioden för datahämtning. En sådan ytterligare tjänst som den ursprungliga leverantören tillhandahåller hindrar inte uppsägningen av det ursprungliga avtalet, och tillhandahållandet av tjänsten skulle baseras på ett nytt eller ändrat avtal.

— Ett tidsbegränsat avtal löper ut innan bytet har skett eller slutförts (händelse D)

Exempel på händelse D: Ett exempel på denna situation kan vara när kunden inte lämnar sitt meddelande i tillräckligt god tid. I detta fall har data inte överförts till destinationsleverantören på den dag då avtalet med den ursprungliga leverantören löper ut.

Parterna bör vara medvetna om att tjänsterna kan komma att avbrytas under bytet. I detta fall gäller den allmänna klausulen om avbrott i tjänsterna som ingår i avtalet.
Undantag för vissa skräddarsydda tjänster finns. Se förklaringen som medföljer standardavtalsklausulerna om byte och utträde.

1. **Uppsägning**

1.1. **Uppsägningsförfarande**

1.1.1. Avtalet anses ha upphört mellan parter när någon av följande händelser inträffat:

(a) I tillämpliga fall, när bytet har slutförts framgångsrikt. Om bytet genomförs framgångsrikt före avtalets avtalade löptid, kommer de avgifter för förtida uppsägning som anges i detta avtal att tillämpas.

(b) Vid utgången av den maximala uppsägningstiden om kunden inte vill byta leverantör utan radera sina exporterbara data och digitala tillgångar när tjänsten upphör.

1.1.2. Om avtalet innehåller villkor avseende uppsägning som omfattas av tillämplig lag, såsom

(a) en part ansöker om betalningsinställelse eller en part har försatts i konkurs,

(b) en part inte i tid har fullgjort någon skyldighet som följer av avtalet och som leder eller kan leda (antingen enligt avtal eller enligt lag) till att avtalet sägs upp,

(c) en part har genomgått en förändring av ägande eller kontroll som, enligt avtal eller lag, leder eller kan leda till att avtalet sägs upp,

(d) avtalet förklaras ogiltigt på grund av brott mot eller förändring av tillämplig tvingande lag, eller

(e) någon annan situation som, enligt avtal eller lag, leder eller kan leda till att avtalet sägs upp;

även om det under bytet uppstår någon grund för uppsägning, kommer avtalet och de avtalade tjänsterna och funktionerna inte att sägas upp eller upphöra att gälla innan bytet har slutförts (se klausul 1.1.1 a) eller vid utgången av den maximala uppsägningstiden, om kunden endast önskar radera sina exporterbara data och digitala tillgångar vid uppsägningen av tjänsten (se klausul 1.1.1 b), om inte annat föreskrivs i tvingande lag. Detta påverkar inte andra rättigheter eller rättsmedel som en part har gentemot den andra parten. Detta gäller även om bytet påbörjas efter att leverantören har lämnat in en uppsägning av avtalet.

1.1.3. Utan att det påverkar andra rättsmedel som är tillgängliga enligt tillämplig lag, kommer avtalet inte att sägas upp eller upphöra att gälla innan bytet har slutförts framgångsrikt, eller innan ett relevant beslut har fattats av en behörig domstol eller en överenskommelse har träffats mellan parterna.

1.2. **Uppsägning efter slutfört byte**

1.2.1. Avtalet sägs inte upp förrän bytet har slutförts. Så snart kunden meddelar leverantören att bytet har slutförts framgångsrikt, meddelar leverantören utan oskäligt dröjsmål kunden om att avtalet har upphört.

1.2.2. Om kunden inte meddelar leverantören om att bytet har genomförts eller inte, medan leverantören har berättigade skäl att tro att bytet har slutförts framgångsrikt av kunden, kan leverantören skicka en begäran till kunden om bekräftelse på att bytet har slutförts framgångsrikt. Om kunden inte bekräftar att bytet har slutförts framgångsrikt inom 30 arbetsdagar från sådan begäran, anses bytet inte ha slutförts framgångsrikt och avtalet upphör inte utan fortsätter att gälla enligt befintliga villkor.

1.3. **Uppsägning utan byte**

1.3.1. Om kunden inte vill byta utan radera sina exporterbara data och digitala tillgångar vid uppsägningen av tjänsten, enligt vad som anges i klausul 1.1.1 b, kan detta endast ske och anses vara genomfört om

(a) den [maximala] överenskomna uppsägningstiden har löpt ut och

(b) kunden uttryckligen har begärt att leverantören ska radera data, och data har raderats och detta har bekräftats av leverantören,

(c) leverantören vid utgången av den överenskomna uppsägningstiden har meddelat kunden att avtalet har upphört.

Andra scenarier [valfria klausuler som ska beaktas]

1.4. **Förlängd datalagring**

1.4.1. Vid övergångsperiodens slut kan kunden besluta att inte radera alla sina exporterbara data och digitala tillgångar vid slutet av den [minsta]/överenskomna perioden för datahämtning och att säkerställa att de kommer att vara tillgängliga, inklusive för att tillhandahålla en tjänst med begränsad funktionalitet, under en angiven förlängd period.

1.4.2. I detta fall kommer kunden och leverantören antingen överens om i) att ändra det befintliga avtalet så att det omfattar den förlängda perioden för datahämtning, eller ii) att ingå ett nytt avtal för tjänster med begränsad funktionalitet.

1.5. **Upphörande av ett tidsbegränsat avtal före byte**

1.5.1. Om avtalet ingicks för en bestämd tid och i) avtalets giltighetstid löper ut innan bytet är slutfört, och ii) kunden inte har begärt att kundens exporterbara data och digitala tillgångar ska raderas,

(a) börjar övergångsperioden den dag avtalet löper ut; leverantören ger rimligt bistånd enligt vad som anges i standardavtalsklausulerna om byte och utträde,

(b) gäller klausul 1.2 när bytet har slutförts framgångsrikt, och

(c) gäller klausul 1.7 under alternativ A eller klausul 2.6 under alternativ B i standardavtalsklausulerna om byte och utträde när bytet inte har slutförts framgångsrikt.

1.6. **Meddelanden**

Parterna är överens om att alla meddelanden mellan dem avseende dessa klausuler om uppsägning ska ske [*parterna fyller i valt kommunikationsmedel, inklusive lämpliga elektroniska medel*].

1.7. **Prioritetsordning**

I händelse av konflikt eller inkonsekvens mellan dessa klausuler om uppsägning och andra tillämpliga avtalsvillkor, bestämmelser eller andra tillämpliga avtal relaterade till uppsägning av avtalet som ligger till grund för tillhandahållandet av databehandlingstjänster, ska dessa klausuler ha företräde.

BILAGA VIII

STANDARDAVTALSKLAUSULER

om säkerhet och driftskontinuitet

I skäl 94 i förordning (EU) 2023/285 (nedan kallad *dataförordningen*) anges att en hög säkerhetsnivå bör upprätthållas under hela bytesprocessen och att leverantören ska iaktta vederbörlig omsorg för att upprätthålla driftskontinuiteten och säkerställa tillhandahållandet av de funktioner eller tjänster som omfattas av avtalet, samt tillhandahålla tydlig information om kända risker för kontinuiteten.

Dataförordningen fastställer skyldigheter för leverantören att säkerställa en hög säkerhetsnivå och driftskontinuitet i samband med bytesprocessen. Detta gäller särskilt säkerheten för data under överföringen och den fortsatta säkerheten för data under perioden för datahämtning (artikel 25.2 a iv i dataförordningen). Även om säkerhet och driftskontinuitet i allmänhet ingår i databehandlingsavtalet och andra avtalsdokument, fokuserar dessa standardavtalsklausuler på säkerhet och driftskontinuitet i samband med bytes- och utträdesprocessen i enlighet med de rättigheter och skyldigheter som införs genom dataförordningen.

Dessa standardavtalsklausuler kombinerar klausuler om specifika frågor om säkerhet och driftskontinuitet under hela bytesprocessen på grund av likheterna mellan säkerhet och driftskontinuitet vad gäller sammanhang och andemening. Även om bestämmelser om säkerhet och driftskontinuitet ingår i tjänsteavtalet finns det vissa särdrag i samband med bytesprocessen som måste beaktas.

Bytesprocessen kan medföra särskilda säkerhetsrisker som kan uppstå under olika faser av bytet med avseende på olika aspekter som kräver särskild uppmärksamhet, såsom

i. databehandling,
ii. identitetshantering och åtkomstkontroll,
iii. dataöverföring,
iv. datahämtning,
v. fortlöpande datakonfidentialitet, dataintegritet och datatillgänglighet, och
vi. andra risker relaterade till förberedelserna för och genomförandet av ett effektivt byte.

Likaså förtjänar särskilda risker för driftskontinuiteten i samband med bytet särskild uppmärksamhet och hänsyn. Dessa risker kan avse

i. upprätthållande av driftskontinuiteten för att säkerställa en hög nivå av tjänstesäkerhet,
ii. fortsatt tillhandahållande av tjänsterna enligt avtalet,
iii. tillhandahållande av tydlig information om kända risker för kontinuiteten i tillhandahållandet av tjänsterna.

I detta avseende ålägger artikel 25.2 a ii i dataförordningen leverantören att iaktta vederbörlig omsorg för att upprätthålla driftskontinuiteten och säkerställa tillhandahållandet av de funktioner eller tjänster som omfattas av avtalet. Leverantören är också skyldig att tillhandahålla tydlig information om kända risker för kontinuiteten i tillhandahållandet av funktionerna eller tjänsterna från den ursprungliga leverantören av databehandlingstjänster (artikel 25.2 a iii i dataförordningen).

Riskbaserad säkerhet och driftskontinuitet: När standardavtalsklausulerna innehåller avtalsvillkor innebär en riskbaserad och allomfattande strategi för säkerhet en dynamisk och kontextuell strategi för tillämpliga tjänster och implementeringsmodeller samt relaterad användning, behov och risker. Det åligger kunden och leverantören att gemensamt identifiera, komma överens om, genomföra och övervaka relaterade åtgärder och kontroller för att säkerställa förbättrad övergripande motståndskraft och integritet för tjänsten.

Särskild uppmärksamhet måste till exempel ägnas åt kontinuerliga lämpliga och ansvariga nivåer av

i. dataintegritet,
ii. motståndskraft mot alla kända sårbarheter när data görs tillgängliga för hämtning,
iii. krypteringssignaturer,
iv. speciell åtkomsthantering med flera faktorer,
v. identitetsverifiering, inklusive auktorisering,

vi. säkerhet för webbplats, portal, plattform och relaterade gränssnitt för applikationsprogrammering (API),
vii. säkerhet på leverantörssidan,
viii. tillhandahållande och säkerställande av kundsidan, inklusive säkerheten hos relevanta destinationsleverantörer,
ix. nätverksaktivitet,
x. råstyrkeregistrering,
xi. transportlagersäkerhet (TLS) och annan säkerhet under överföring,
xii. skydd mot samordnade överbelastningsattacker (DDoS) och
xiii. kraftfulla policyer och rutiner för radering av data.

Leverantören ska kunna visa, till förmån för kunden, att de tekniska, operativa och organisatoriska åtgärderna för säkerhet och dataskydd tillhandahålls på ett kontinuerligt och lämpligt sätt.

Denna princip liknar strukturen och tillvägagångssättet i i) artikel 25 i dataskyddsförordningen respektive artikel 32 i dataskyddsförordningen [förordning 2016/679], ii) NIS 2-direktivet [EUR-Lex] och iii) certifieringssystemet för cybersäkerhet enligt förordningen om cybersäkerhet (EU) 2019/881.

Exempel på vad leverantören bör visa upp är
i. interna policyer för säkerhet, säkerhetsövervakning och hantering av säkerhetsöverträdelser eller andra incidenter,
ii. efterlevnad av vissa öppna, icke-proprietära standarder som vanligtvis används inom den relevanta sektorn,
iii. certifiering eller annan säkerhet som överensstämmer med, eller på annat sätt följer, antingen relevant tillämplig nationell lagstiftning eller relevanta europeiska certifieringssystem för cybersäkerhet som utvecklats enligt förordning (EU) 2019/881 (förordningen om cybersäkerhet), eller
iv. tekniska standarder för tillsyn, om och där det är tillämpligt i den eller de relevanta sektorerna.

Riskbaserade regler: För många leverantörer som är verksamma i EU, liksom för vissa kunder, kan vissa riskbaserade regler vara tillämpliga. Detta leder i allmänhet till ökade säkerhetskrav och ansvar, där överträdelser och andra incidenter får allvarligare rättsliga, reputationsmässiga och andra konsekvenser. Det rekommenderas därför starkt att dessa riskbaserade regler beaktas innan ett tjänsteavtal ingås och under dess genomförande.

Några exempel på riskbaserade regler som kan vara tillämpliga är NIS 2-direktivet (NIS 2), direktivet om kritiska entiteters motståndskraft (CER), förordningen om digital operativ motståndskraft (DORA), cyberresiliensförordningen, förordningen om cybersäkerhet och den allmänna dataskyddsförordningen samt eventuella regler enligt nationell lagstiftning.

Dessa standardavtalsklausuler använder termen *incident* i relation till både säkerhet och driftskontinuitet (se avsnittet Definitioner).

Klausul 1.4 omfattar till exempel även anmälningar enligt artikel 33 i dataskyddsförordningen och artikel 23 i NIS 2-direktivet.

Andra standardavtalsklausuler som rekommenderas av kommissionen finns bifogade och täcker andra specifika ämnen än säkerhet och driftskontinuitet. Parterna uppmuntras att överväga att använda även dessa andra klausuler, eftersom de har utformats för att vara samstämmiga och förstärka varandra.

1. **Säkerhet och driftskontinuitet**

1.1. **Allmänt**

1.1.1. Leverantören åtar sig att tillämpa de mest lämpliga tekniska och organisatoriska åtgärderna för att säkerställa att nivån på säkerhet och motståndskraft står i proportion till de risker som tjänsterna medför och deras avsedda och rimligt förutsebara användning med avseende på bytesprocessen.

1.1.2. Dessutom åtar sig leverantören att förhindra störningar i tjänsterna och upprätthålla kontinuiteten i tjänsterna under bytesprocessen. Detta omfattar att ha och upprätthålla adekvat kontinuitetshantering som omfattar beredskapsplanering och åtgärder för katastrofåterhämtning baserade på etablerad bästa praxis och marknadsstandarder. Dessa åtgärder måste hållas uppdaterade och regelbundet granskas och testas av leverantören.

1.2. **Säkerhet**

1.2.1. Utöver klausul 1.1.1 måste leverantören vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att en hög säkerhetsnivå upprätthålls under bytesprocessen. Detta avser i synnerhet säkerheten för data under överföringen och fortsatt säkerhet för data under perioden för datahämtning.

1.2.2. Leverantören måste vidta lämpliga tekniska och organisatoriska åtgärder för att under bytet upprätthålla en säkerhetsnivå som står i proportion till risknivån. Detta omfattar relevanta risker relaterade till säkerheten vid databehandling, identitetshantering och åtkomstkontroll, dataportabilitet, datahämtning, fortlöpande datakonfidentialitet, dataintegritet och datatillgänglighet samt alla andra risker relaterade till ett effektivt byte.

1.2.3. Åtgärderna i klausulerna 1.1.1 och 1.2.1 måste åtminstone utan begränsning säkerställa

(a) fortlöpande datakonfidentialitet, dataintegritet och datatillgänglighet och motståndskraft hos tjänsterna, exporterbara och digitala tillgångar,

(b) återställande av tillgängligheten och integriteten hos data och åtkomst till dem inom rimlig tid i händelse av en incident, och

(c) kontinuerlig övervakning samt regelbundna tester, bedömningar och utvärderingar av effektiviteten hos tekniska och organisatoriska åtgärder för att säkerställa säkerheten hos tjänsterna, exporterbara data och digitala tillgångar.

1.3. **Driftskontinuitet**

1.3.1. Utöver klausul 1.1.2 måste leverantören i synnerhet

(a) iaktta vederbörlig omsorg för att upprätthålla driftskontinuitet och fortsätta att tillhandahålla tjänster enligt avtalet, och

(b) tillhandahålla tydlig information om kända risker för kontinuiteten i tillhandahållandet av tjänsterna.

1.4. **Meddelanden**

1.4.1. Parterna är överens om att alla meddelanden mellan dem avseende dessa klausuler om säkerhet och driftskontinuitet ska ske [*parterna fyller i valt kommunikationsmedel, inklusive lämpliga elektroniska medel*].

1.4.2. Leverantören måste meddela kunden om eventuella incidenter. Leverantören måste meddela utan oskäligt dröjsmål och under alla omständigheter inom 72 (sjuttiotvå) timmar efter att ha fått kännedom om incidenten, såvida inte lagstadgade skyldigheter kräver en varning eller liknande meddelande inom en kortare period.

1.4.3. Leverantörens meddelande måste innehålla den information som kunden behöver för att kunna bedöma konsekvenserna av incidenten. Leverantören måste omedelbart, effektivt, rimligt och utan extra kostnad bistå och samarbeta med kunden (inklusive med tredje parter som bemyndigats av kunden) när det gäller alla utredningsåtgärder som kunden har rätt att vidta i enlighet med tillämplig unionsrätt och nationell rätt.

1.4.4. Om leverantören påverkas eller sannolikt kommer att påverkas av en incident måste leverantören vidta de mest lämpliga åtgärder som krävs för att minimera incidentens inverkan och förhindra att den upprepas. Detta påverkar inte andra rättigheter som kunden kan ha enligt avtalet eller enligt tillämplig unionsrätt och nationell rätt.

1.5. **Övrigt**

1.5.1. På kundens begäran ska leverantören utan oskäligt dröjsmål tillhandahålla kunden en sammanfattning av de viktigaste delarna av leverantörens säkerhetsåtgärder och relaterad säkerhetshantering, samt av dess driftskontinuitet och relaterad beredskapshantering och av alla väsentliga förändringar av något av ovanstående.

1.5.2. På kundens begäran måste leverantören utan oskäligt dröjsmål förse kunden med ytterligare information som kompletterar ovanstående sammanfattning, såsom testresultat och verifierbar försäkran. I detta fall kan leverantören kräva att kunden undertecknar ett sekretessavtal innan sådan information delas. Detta sekretessavtal måste dock innehålla sedvanliga undantag och får inte påverka övriga villkor i detta stycke, avtalet eller tillämplig unionsrätt och nationell rätt. Leverantören har rätt att begära att uppgifterna endast delas på behovsbasis, inklusive med dess utsedda leverantör(er) eller andra relevanta tredjepartsleverantörer till kunden.

Sådana sedvanliga undantag inkluderar alla (relevanta delar av) uppgifter i) som redan är offentliga, ii) som kunden är skyldig att lämna ut när det är obligatoriskt att göra det a) enligt tillämplig lag eller b) enligt någon statlig eller annan tillsynsmyndighet (de två senare inkluderar utan begränsning domstolsbeslut, dataskyddsförordningen, NIS 2-direktivet).

1.6. **Prioritetsordning**

Utan att det påverkar standardavtalsklausulerna enligt dataskyddsförordningen ska dessa klausuler ha företräde i händelse av konflikt eller inkonsekvens mellan dessa klausuler om säkerhet och driftskontinuitet och andra tillämpliga avtalsvillkor, bestämmelser eller andra tillämpliga avtal relaterade till säkerhet och driftskontinuitet.

BILAGA IX

STANDARDAVTALSKLAUSULER

om icke-spridning

Databehandlingsavtal består ofta av olika kompletterande dokument som hänvisar till ytterligare material och information som kan vara spridda över olika register. Detta gör det svårt för potentiella kunder att hitta all information de behöver för att kunna bedöma parternas avtalsenliga och rättsliga skyldigheter och deras konsekvenser.

I samband med bytet är transparens mycket viktigt. En potentiell kund behöver enkel åtkomst till relevant uppdaterad information, dokument, material och kontaktuppgifter, även innan avtalet med leverantören ingås. Standardavtalsklausulerna om icke-spridning säkerställer symmetri i fråga om information och kommunikation.

Dessa standardavtalsklausuler underlättar för både kunden och leverantören att få enkel och praktisk åtkomst till relevant uppdaterad information, dokument, material och kontaktuppgifter. De syftar till att skapa en miljö präglad av transparens mellan parterna och att säkerställa att det inte finns några avtalsmässiga hinder för byte, genom att kunden kan hitta all relevant och uppdaterad information om sina rättigheter och skyldigheter i avtalet. Detta kommer att bidra till en rättvis och balanserad rättslig relation mellan kunden och leverantören och, i allmänhet, till avtalsmässig rättvisa, såsom förespråkas i förordning (EU) 2023/285 (nedan kallad *dataförordningen*).

Andra standardavtalsklausuler som rekommenderas av kommissionen finns bifogade och täcker andra specifika ämnen än icke-spridning. Parterna uppmuntras att överväga att använda även dessa andra klausuler, eftersom de har utformats för att vara samstämmiga och förstärka varandra.

1. Icke-spridning

1.1. Inledande villkor och arrangemang

1.1.1. Leverantören säkerställer att alla avtalsvillkor är lätt åtkomliga och kontinuerligt tillgängliga för kunden a) på en särskild säker plats online, och b) i ett begripligt format som är läsbart för både människor och maskiner. Dessutom säkerställer leverantören att avtalsvillkoren kan laddas ned eller på annat sätt exporteras av kunden på ett fullständigt och strukturerat sätt.

1.1.2. Avtalsvillkoren måste minst innehålla följande:

(a) **Namn och adress:** Leverantörens fullständiga officiella företagsnamn som juridisk person, inklusive, utan begränsning, dess officiella juridiska form, nationella registreringsnummer, fullständiga officiella adress och momsregistreringsnummer.

(b) **Uppdaterat avtal:** Det aktuella, tidsstämplade (och där så är möjligt, undertecknade) avtalet, inklusive alla villkor, accepterade erbjudanden, bestämmelser, policyer, information, dokumentation, scheman, underlag och bilagor som är tillämpliga mellan leverantören och kunden.

(c) **Historik:** Historiken över de tidsstämplade avtalen, om möjligt tillsammans med eventuella tilläggsvillkor, inklusive policyer, information, dokumentation, scheman, underlag, bilagor eller annat som har varit tillämpligt mellan leverantören och kunden,

i) inklusive bevis på tillåtna ensidiga ändringar och respektive tillåtna ensidiga ändringars datum för ikraftträdande enligt standardavtalsklausulerna om icke-ändring.

För tillåtna ensidiga ändringar och respektive tillåtna ensidiga ändringars datum för ikraftträdande, se standardavtalsklausulerna om icke-ändring.

(d) **Databehandling och leveranssystem:** Den aktuella historiska dokumentationen och detaljerade förteckningen över underleverantörer, databehandlare och/eller andra relevanta intressenter i leveranskedjan, inklusive namn och adresser enligt klausul 1.1.2 a ovan.

(e) **Kontaktuppgifter:** Leverantörens aktuella kontaktuppgifter, inklusive uppgifter om funktionerna för den primära kontaktpersonen, den primära tekniska kontaktpersonen och den primära kontaktpersonen för avtal och administration, inklusive respektive funktionstitlar, telefonnummer och e-postadresser som parterna har kommit överens om.

(f) **Rapportering av operativ prestanda:** Om det är tekniskt genomförbart, en aktuell och historisk översikt över leverantörens rapportering av operativ prestanda för den tillhandahållna tjänsten och andra skyldigheter enligt avtalet.

(g) **Meddelande:** Alla juridiska och andra relevanta tidsstämplade meddelanden mellan parterna eller till en part som rör avtalsvillkoren enligt klausul 1.1.2 a och b.

I flera situationer ålägger dataförordningen leverantören att tillhandahålla erforderlig information till kunden. Dessa skyldigheter återspeglas i de relevanta standardavtalsklausulerna. Exempelvis ingår information om tillgängliga förfaranden för byte och överföring av data (artikel 26 i dataförordningen) i standardavtalsklausulerna om byte och utträde. Skyldigheten att tillhandahålla tydlig information om kända risker för fortsatt tillhandahållande av funktioner/tjänster återspeglas i standardavtalsklausulerna om säkerhet och driftskontinuitet samt i standardavtalsklausulerna om byte och utträde.

1.2. **Prioritetsordning**

I händelse av konflikt eller inkonsekvens mellan dessa klausuler om icke-spridning av tillämplig avtalsdokumentation och andra tillämpliga avtalsvillkor, bestämmelser eller andra tillämpliga avtal relaterade till ämnet för dessa klausuler, ska dessa klausuler ha företräde.

BILAGA X

STANDARDAVTALSKLAUSULER

om ansvar

Även om en klausul om ansvar vanligtvis ingår i det allmänna avtalet mellan kunden och leverantören, återspeglar bestämmelserna i dessa standardavtalsklausuler om ansvar andemeningen i förordning (EU) 2023/2854 (nedan kallad *dataförordningen*) när det gäller vikten av rättvisa, rimliga och icke-diskriminerande rättigheter och skyldigheter, och kan som sådan vara ett användbart komplement till standardbestämmelserna i ett avtal om ansvar.

Det rekommenderas därför att en sådan klausul inkluderas, eftersom den är viktig för balansen i avtalsförhållandet mellan parterna och ger incitament för att följa de rättigheter och skyldigheter som parterna har kommit överens om. Särskilt små och medelstora företag och andra organisationer kan finna dessa standardavtalsklausuler användbara när de kommer överens om ansvarsbestämmelser i sina avtal. Kunden och leverantören är fria att komma överens om ytterligare rättigheter och skyldigheter i sitt avtal. Användningen av denna klausul befriar inte parterna från att säkerställa efterlevnaden av tillämpliga tvingande bestämmelser i unionsrätt eller nationell rätt och anpassa dem i enlighet därmed.

Innan ett avtal ingås kan kunden undersöka försäkringsmarknaden för att hitta den försäkringsprodukt som bäst passar dennes behov. Det rekommenderas att rådfråga en expert som är specialiserad på försäkringar.

Andra standardavtalsklausuler som rekommenderas av kommissionen finns bifogade och täcker andra specifika ämnen än ansvar. Parterna uppmuntras att överväga att använda även dessa andra klausuler, eftersom de har utformats för att vara samstämmiga och förstärka varandra.

Obegränsat ansvar

Som regel bör varje part i avtalet ha obegränsat ansvar i fall av uppsåt, avsiktlig försummelse eller grov oaktsamhet, inklusive en parts åsidosättande av skyldigheten att behandla den andra partens data konfidentiellt eller skyldigheten att inte använda data för andra ändamål än de som uttryckligen överenskommits mellan parterna.

I standardavtalsklausulerna rekommenderas att man skiljer mellan fall där åsidosättandet är uppsåtligt och fall där det orsakas av avsiktlig försummelse, och att man tydligt anger att alla uppsåtliga handlingar omfattas, oavsett vilken lag som reglerar avtalet. I vissa jurisdiktioner kan avsiktlig försummelse vara synonymt med uppsåt. I sådana fall kan parterna besluta att inte göra någon åtskillnad mellan avsiktlig försummelse och uppsåt.

Undantag från obegränsat ansvar

Databehandlingstjänster som tillhandahålls som icke-produktionsversioner för testnings- och utvärderingsändamål och under en begränsad tidsperiod (artikel 31.2 i dataförordningen) är vanligtvis inte avsedda för behandling av känsliga data (t.ex. företagshemligheter, personuppgifter eller faktiska produktionsdata). Sådana icke-produktionsversioner är i allmänhet inte tillräckligt utvecklade för sådan behandling och saknar de funktioner, kontroller och konfigurationer som rimligen kan förväntas i produktionsversionen. Kunden avråds starkt från att behandla faktiska produktionsdata i sådana icke-produktionsversioner. Dessa standardavtalsklausuler föreslår att om kunden beslutar att göra detta, sker det på egen risk och att leverantören inte är ansvarig om en överträdelse av datakonfidentialiteten inträffar i sådana fall. I denna situation kan särskilda ansvarsarrangemang som parterna har kommit överens om tillämpas.

På samma sätt förutsätter dataförordningen situationer där vissa skyldigheter inte gäller för tjänster där de flesta huvudfunktionerna har skräddarsytts, där alla komponenter har utvecklats för en enskild kund eller för tjänster som tillhandahålls i en icke-produktionsmiljö. Följaktligen måste ansvaret för dessa fall också uttryckligen avtalas.

Begränsat ansvar

Det är gängse affärspraxis att parterna i vissa fall kommer överens om att begränsa sitt ansvar (särskilt leverantörens). Dessa standardavtalsklausuler föreslår tre huvudsakliga alternativ för att begränsa ansvaret:

— **Alternativ A:** Ansvaret är begränsat till det belopp som parterna fastställt på grundval av en riskbedömning. Enligt detta alternativ utför båda parter en riskbedömning och lämnar sina slutsatser till den andra parten i förhandlingsfasen. Den andra parten kan avvisa den mottagna riskbedömningen. Om riskbedömningen avvisas kan parterna tillämpa ett av de andra alternativen för att begränsa ansvaret.

Det kan förekomma förändringar i volymen av tjänster som erhålls från leverantören, liksom en förändring av omfattningen (tillägg av nya tjänster eller borttagande av vissa tjänster). Detta kan kräva ändringar av riskbedömningen och parterna bör anpassa ansvarsbegränsningen så att den återspeglar den faktiska risksituationen. Parterna uppmanas att kontrollera exemplet på mallen för riskbedömning i alternativ A så att de är medvetna om de risker som är förknippade med databehandlingstjänster för just deras verksamhet.

— **Alternativ B**: Ansvaret är begränsat till direkta skador. Följdskador såsom utebliven vinst eller uteblivna besparingar är undantagna. Detta alternativ kan också kombineras med alternativ A och C (dvs. begränsa ansvaret till direkta skador, men inte högre än ett belopp som parterna fastställt antingen efter en riskbedömning eller på annan grund).

— **Alternativ C**: Parternas ansvar är begränsat till ett i förväg överenskommet högsta belopp, som kan beräknas till exempel på grundval av i) motsvarande enstaka/flera årsavgifter (betalda och utestående) som kunden betalar till leverantören, ii) den försäkring som leverantören tecknat för tjänsterna, iii) det högsta belopp som täcks av leverantörens allmänna ansvarsförsäkring, eller iv) en kombination av olika formler, t.ex. en formel kopplad till tjänsternas penningvärde multiplicerat med ett belopp som motsvarar de totala årliga avgifterna (antingen betalda eller utestående/förfallna enligt avtalet) för tjänsterna.

Skadeersättning: Dessa standardavtalsklausuler innehåller inga bestämmelser om skadeersättning. Parterna uppmanas att överväga om och, i så fall, i vilken utsträckning en part kan behöva ersätta och hålla den andra parten skadeslös från eventuella anspråk från tredje part som orsakats av eller är relaterade till ett väsentligt brott mot skyldigheterna enligt avtalet genom handlingar eller underlåtenhet från den ansvariga partens, dess anställdas, representanters eller underleverantörers sida. För kunder kan ersättningen till exempel gälla leverantörens åsidosättande av sina skyldigheter avseende konfidentialitet, icke-användning eller intrång i tredje parts immateriella rättigheter. För leverantörer kan ersättningen täcka kundens intrång i tredje parts immateriella rättigheter eller tredje parts anspråk på leverantören i samband med att kunden är värd för olagligt innehåll.

1. **Ansvar**

1.1. **Obegränsat ansvar**

1.1.1. Vid åsidosättande av skyldigheterna enligt detta avtal som begåtts med uppsåt eller orsakats av avsiktlig försummelse eller grov oaktsamhet, är den part som åsidosatt skyldigheterna ansvarig för alla skador, med förbehåll för klausul 1.2 nedan. [ALTERNATIV] [Med undantag för vad som anges i klausul 1.2 är leverantören obegränsat ansvarig för alla skador som orsakas kunden genom brott mot konfidentialiteten för kundens data som behandlas enligt detta avtal.]

1.1.2. Vid överträdelse av skyldigheten att inte använda en parts data för andra ändamål än de som uttryckligen överenskommits mellan parterna är den part som begått överträdelsen ansvarig för alla skador utan begränsning.

Avsikten med alternativet i klausul 1.1.1 är att garantera konfidentialiteten för all kunddata i enlighet med rättigheterna och skyldigheterna avseende konfidentialitet och i den utsträckning som överenskommits i avtalet. Enligt tillämplig lag (till exempel dataskyddsförordningen, NIS 2-direktivet osv.) kan en mottagare av konfidentiell information ha vissa skyldigheter att lämna ut viss information till vissa personer/organisationer för ändamål som överenskommits och uttryckligen beskrivits i avtalet.

1.2. **Undantag från obegränsat ansvar**

1.2.1. Om parterna kommer överens om obegränsat ansvar enligt klausul 1.1.1, gäller leverantörens obegränsade ansvar inte för kunddata i en icke-produktionsversion av leverantörens databehandlingstjänster.

Se artikel 31.2 i dataförordningen och den förklarande anmärkningen ”Undantag från obegränsat ansvar” i dessa standardavtalsklausuler.

1.2.2. Leverantören är inte ansvarig för

(a) skyldigheter som inte är tillämpliga på databehandlingstjänster enligt i) artikel 23 d i dataförordningen (uppnå funktionell likvärdighet), ii) artikel 29 (gradvis avskaffande av bytesavgifter), eller iii) artiklarna 30.1 och 30.3 i dataförordningen (tekniska aspekter av byte) om de flesta av de viktigaste funktionerna i leverantörens databehandlingstjänster är skräddarsydda för att tillgodose kundens specifika behov eller om alla komponenter har utvecklats för kundens ändamål, och om dessa databehandlingstjänster inte erbjuds i bred kommersiell skala via tjänstekatalogen för databehandlingstjänster. Undantaget gäller om leverantören före ingåendet av avtalet om databehandlingstjänster har informerat kunden om att ovanstående bestämmelser i dataförordningen inte gäller för nämnda tjänster,

(b) en överträdelse av skyldigheterna i samband med byte mellan databehandlingstjänster till databehandlingstjänster som tillhandahålls som en icke-produktionsversion för testnings- och utvärderingsändamål och under en begränsad tidsperiod.

1.3. **Begränsat ansvar**

Alternativ A: Belopp som fastställs genom en riskbedömning

1.3.1. Parterna är överens om att begränsa sitt ansvar vid vårdslös överträdelse av skyldigheter enligt detta avtal till ett belopp på […] per händelse, inklusive när en serie sammanhängande händelser betraktas som en enda händelse. Beloppet fastställs av den skadelidande parten i god tro på grundval av en riskbedömning eller andra uppskattningar som parterna har kommit överens om i bilaga 1 (Mall för riskbedömning). Riskbedömningen genomförs och lämnas till den andra parten [… dagar] före avtalets ingående. Om riskbedömningen inte avvisas av den andra parten ingås avtalet på denna grund.

Parterna kan när som helst komma överens om att ompröva riskerna för att återspegla förändringar i risksituationen med avseende på tjänsterna. För detta kan de använda mallen i exemplet [Mall för riskbedömning]. Om omprövningen leder till en ökning eller minskning av risken för parten, kan den parten begära att förhandla om ansvarsbegränsningen för tjänsterna för att återspegla förändringen i den risk som är förknippad med dem eller ytterligare villkor som bör uppfyllas, vilket kan omfatta prissättning eller ändringar av det överenskomna servicenivåavtalet. Parterna kan komma överens om att, om inget avtal nås inom [tre månader från partens begäran], den ursprungligen överenskomna ansvarsbegränsningen ska förbli oförändrad.

Alternativ B: Direkta skador

1.3.2. Parterna är överens om att begränsa sitt ansvar vid vårdslös överträdelse av skyldigheter enligt detta avtal till eventuella direkta skador som orsakats.

1.3.3. Direkta skador omfattar även i) kostnader som uppkommit för att fastställa orsaken till och omfattningen av skadorna, ii) kostnader som den skadelidande parten ådragit sig för att förhindra eller begränsa direkta skador, förutsatt att dessa kostnader faktiskt lett till att skadorna förhindrats eller begränsats, iii) skador på grund av skadade, otillgängliga eller förlorade data, och iv) kostnader som en part ådragit sig för att säkerställa att tjänsterna uppfyller de användningsnivåer som överenskommits i avtalet, om den andra parten inte har åtgärdat sådan överträdelse inom den överenskomna tiden.

1.3.4. Om en serie sammanhängande händelser betraktas som en enda händelse, är den ena partens sammanlagda ansvar gentemot den andra parten för sådana direkta skador som anges i föregående mening begränsat till ett belopp på […].

Alternativ C: Högsta belopp

1.3.5. Parterna är överens om att begränsa sitt ansvar vid vårdslös överträdelse av skyldigheter enligt detta avtal, inklusive när en serie sammanhängande händelser betraktas som en händelse, till ett högsta belopp på […].

1.4. **Meddelanden**

Parterna är överens om att alla meddelanden mellan dem avseende dessa klausuler om ansvar ska ske [parterna fyller i valt kommunikationsmedel, inklusive lämpliga elektroniska medel].

1.5. **Prioritetsordning**

I händelse av konflikt eller inkonsekvens mellan dessa klausuler om ansvar och andra tillämpliga avtalsvillkor, bestämmelser eller andra tillämpliga avtal relaterade till ansvar inom ramen för dessa klausuler, ska dessa klausuler ha företräde.

Tillägg 1 –

Mall för riskbedömning

För att fastställa de risker som är förknippade med tjänsten genomför en part en bedömning där hänsyn tas till de specifika riskerna för försumlig underlåtenhet att fullgöra sina skyldigheter enligt avtalet från den andra partens sida.

Denna riskbedömning måste göras i god tro. Den bör på ett realistiskt sätt återspegla potentiella skador. Om de uppskattade beloppen är för låga utesluts ansvar för högre skadestånd. Om de uppskattade beloppen är för höga kan den andra parten vägra att acceptera ansvar eller kräva högre kostnader.

Ytterligare risker kan inkluderas vid behov.

Riskbeskrivning		Skadeuppskattning
Avbrott i verksamheten Förlust av omsättning orsakad av avtalsbrott. Eventuella driftstopp och deras inverkan på partens verksamhet eller drift kan beaktas.	EUR	
Dataåterställning Förutsatta kostnader för återställning av förlorade, otillgängliga eller skadade data. Parterna kan vara skyldiga att vidta åtgärder för att minska sina risker, t.ex. genom att ha säkerhetskopior av data hos en annan leverantör eller i sina lokaler.	EUR	
Statliga böter Statliga böter mot företag är till exempel böter för brott mot dataskyddslagar eller regleringsbestämmelser som är en följd av leverantörens drift av tjänsten.	EUR	
Förlust av företagshemligheter Röjande av företagshemligheter kan leda till förlust av affärsmöjligheter. Sådana skador kan vara ersättningsgilla enligt lag.	EUR	
Personuppgiftsincidenter och åtgärder för att avhjälpa dessa En personuppgiftsincident kan leda till flera typer av direkta kostnader relaterade till advokatkostnader, rättegångskostnader samt åtgärder för att avhjälpa problem med datakvaliteten i samband med incidenten.	EUR	
Förlust av anseende Parterna kan överväga inverkan på företagets anseende och vilka åtgärder som kommer att krävas (t.ex. reklam och kampanjer för att kompensera för inverkan på anseendet). Sådana kostnader kan vara svåra att få full ersättning för i domstol.	EUR	
Tredje parts ansvar Tredje parts ansvar omfattar potentiellt ansvar, till exempel gentemot leverantörer, kunder, underleverantörer och tredje part.	EUR	
Total risk för potentiella skador (summa)	**EUR**	

Eftersom databehandlingstjänster tillhandahålls på ett skalbart och elastiskt sätt kan både användningen av den tjänst som tillhandahålls av leverantören och ansvarsrisken variera under avtalets löptid, ofta inom ramen för servicenivåavtalen. Vid bedömningen av riskerna vid avtalets ingående eller på återkommande basis rekommenderas parterna att beakta tjänsternas föränderliga karaktär och volym utöver de potentiella maximala teoretiska skadorna. Detta skulle möjliggöra ett mer realistiskt värde för genomsnittlig eller förväntad användning av tjänsten. Parterna bör också anpassa bedömningen till sin interna planering. Alla riskkategorier som anges är inte nödvändigtvis lika tillämpliga på en kund och leverantör eller på en kunds specifika bransch.

BILAGA XI

STANDARDAVTALSKLAUSULER

om icke-ändring

Det är viktigt att parterna kan förlita sig på de avtalsenliga rättigheter och skyldigheter och att dessa rättigheter och skyldigheter inte ändras ensidigt, såvida inte detta sker enligt tydligt och ömsesidigt överenskomna villkor. Detta gäller särskilt små och medelstora företag eller andra organisationer, som kanske inte har tillräckliga resurser för att bedöma de möjliga effekterna av dessa ensidiga ändringar på deras verksamhet och uppdrag. Standardavtalsklausulerna om icke-ändring syftar till att ge parterna större klarhet och förtroende när de kommer överens om villkor som rör ensidiga ändringar. Dessa standardavtalsklausuler behandlar relevanta scenarier och möjliga avtalsvillkor i samband med dessa. De syftar till att säkerställa att sådana ensidiga ändringar inte skadar någon av parternas intressen.

Förfarande för ensidiga ändringar

Som allmän regel kan avtalet (inklusive standardavtalsklausulerna) inte ändras ensidigt av någon av parterna utan måste godkännas av båda parter. Vissa ensidiga ändringar är endast tillåtna under strikta villkor som anges i dessa standardavtalsklausuler. Detta återspeglas i klausulerna 1.1.1–1.1.3 i dessa standardavtalsklausuler.

Dessa standardavtalsklausuler erkänner att leverantören under vissa omständigheter bör kunna föreslå ensidiga ändringar av de tjänster som tillhandahålls. Dessa kallas tillåtna ensidiga ändringar och anges i klausulerna 1.1.3–1.1.6 i dessa standardavtalsklausuler. En tillåten ensidig ändring, eller flera sådana ändringar, kan endast föreslås en gång och ska uppfylla följande villkor:

(1) Den/de förbättrar kundens ställning när det gäller användningen av tjänsten ur ett avtalsmässigt, ekonomiskt, organisatoriskt, operativt, servicenivåmässigt, rättsligt eller annat perspektiv.

(2) Den/de meddelas kunden senast 30 kalenderdagar innan en sådan föreslagen tillåten ensidig ändring träder i kraft för kunden.

Meddelandeperioden ger kunden möjlighet att bedöma informationen samt genomförbarheten och konsekvenserna för kunden och kundens intressenter, system och tjänster.

Andra standardavtalsklausuler som rekommenderas av kommissionen finns bifogade och täcker andra specifika ämnen än icke-ändring. Parterna uppmuntras att överväga att använda även dessa andra klausuler, eftersom de har utformats för att vara samstämmiga och förstärka varandra.

1. **Icke-ändring**

1.1. **Ändring**

1.1.1. Varje ändring av avtalet (*ändring*) måste göras skriftligen, inklusive med lämpliga elektroniska medel, och ska föregås av ömsesidigt samtycke, inklusive med lämpliga elektroniska medel.

1.1.2. Utan hinder av klausul 1.1.1 har leverantören rätt att ändra avtalet om detta krävs för att följa tvingande tillämplig lag som inte redan var i kraft före avtalets ikraftträdande.

1.1.3. Med undantag för vad som anges i klausul 1.1.2 har leverantören endast rätt att föreslå en ensidig ändring av tjänsterna, förutsatt att

(a) sådan ändring är fördelaktig för kundens användning av databehandlingstjänsterna, till exempel genom att den består av väsentliga förbättringar av tjänsten eller är nödvändig av säkerhetsskäl, och

(b) samtliga villkor som anges i klausulerna 1.1.4–1.1.6 (Tillåten ensidig ändring) är uppfyllda.

1.1.4. Ingen föreslagen ensidig ändring enligt klausul 1.1.3 får användas av leverantören för att direkt eller indirekt genomföra eller verkställa retroaktiva ändringar, eller för att ändra klausuler i avtalet som avser en eller flera av följande aspekter:

(a) Val av lag och val av forum.

(b) Ändringar eller förfaranden för att ändra avtalet.

(c) Löptid och uppsägning.

(d) Ansvar.

(e) Konfidentialitet.

(f) Metoder för användning av underleverantörer och metoder för byte av underleverantörer.

(g) Åtkomst- och informationsrättigheter.

(h) Kvalitativa servicenivåmål.

Ändringar av redan överenskomna kvantitativa och kvalitativa mål för tjänsteprestanda inom de överenskomna servicenivåerna med tillhörande påföljder och/eller servicekrediter kan föreslås som en tillåten ensidig ändring enligt klausul 1.1.3.

(i) Prissättningsregler eller andra finansiella regler.

En ändring av de överenskomna avgifterna kan föreslås som en tillåten ensidig ändring enligt klausul 1.1.3, men de underliggande reglerna, såsom metoden för prisindexering, måste i sig vara ömsesidigt överenskomna mellan parterna.

(j) Den plats där data behandlas eller lagras, om denna plats ligger utanför EU.

Ändringar mellan platser inom EU kan avtalas av parterna från början av deras avtalsförhållande eller kan föreslås av leverantören som en tillåten ensidig ändring. Om platsen där data behandlas eller lagras ändras från en plats inom EU till en plats utanför EU eller från en plats utanför EU till en annan plats utanför EU, ska parterna dock gemensamt komma överens om denna ändring.

1.1.5. Vid förslag om tillåten ensidig ändring måste leverantören

(a) meddela kunden senast 30 kalenderdagar innan den föreslagna tillåtna ensidiga ändringen träder i kraft, om inte annat krävs enligt tillämplig lag,

(b) på ett tydligt och begripligt sätt förse kunden med information om bland annat

i) omfattningen, detaljerna och tidsplanen för den föreslagna tillåtna ensidiga ändringen,

ii) varför den föreslagna tillåtna ensidiga ändringen krävs, inklusive med avseende på dess fördelar för kundens användning av databehandlingstjänsterna,

iii) skillnaden mellan den rådande situationen och situationen efter den föreslagna tillåtna ensidiga ändringen. Detta omfattar i synnerhet eventuella konsekvenser för kunden avseende avtal, ekonomi, organisation, drift, servicenivå och efterlevnad av lagar och regler,

Beskrivningen av en sådan skillnad bör ta upp den förväntade situationen med avseende på relevanta typer av befintliga kunder, med beaktande av de kategorier som anges i klausul 1.1.5 b iii. Detta för att säkerställa att de mest sannolika konsekvenserna av en anmäld ensidig ändring är synliga och begripliga för kunden. I detta avseende kräver denna klausul inte att leverantören meddelar en bedömning som är anpassad till enskilda kunder.

iv) den planerade tidsplanen för införande och genomförande, samt det relaterade datumet för ikraftträdande av den föreslagna tillåtna ensidiga ändringen.

1.1.6. Om leverantören uppfyller villkoren i klausul 1.1.5 ska kunden anses ha accepterat den föreslagna tillåtna ensidiga ändringen vid datumet för ikraftträdande av den tillåtna ensidiga ändringen.

1.1.7. Om leverantören bryter mot klausulerna 1.1.2–1.1.5 avseende ändring av avtalet, har kunden rätt att säga upp avtalet utan extra kostnad och att erhålla ersättning för den skada som lidits (inklusive kostnaderna för att byta till en annan leverantör av databehandlingstjänster). Detta påverkar inte kundens övriga rättigheter och rättsmedel, inklusive rätten att begära föreläggande vid behörig domstol för att ålägga leverantören att fortsätta tillhandahålla tjänsterna enligt avtalet och att erhålla ersättning för eventuella skador.

Om leverantörens ändring av avtalet inte är i linje med avtalsbestämmelserna, ska kunden ha rätt att säga upp avtalet, vilket i praktiken också bör innebära att ett meddelande om byte lämnas in för att inleda bytesprocessen (se standardavtalsklausulerna om byte och utträde, alternativ A om parterna har kommit överens om en bytes- och utträdesplan och alternativ B i fall av självbetjäning med automatiserat byte). I sådana fall bör kunden dock ha rätt att få ersättning för den skada som denne lidit genom att ha ”tvingats” byta till en annan leverantör, inklusive de kostnader som denne ådragit sig och andra relaterade skador (se standardavtalsklausulerna om ansvar).

1.2. **Meddelanden**

Parterna är överens om att alla meddelanden mellan dem avseende dessa klausuler om icke-ändring ska ske [*parterna fyller i valt kommunikationsmedel, inklusive lämpliga elektroniska medel*].

1.3. **Prioritetsordning**

I händelse av konflikt eller inkonsekvens mellan dessa klausuler om icke-ändring och andra tillämpliga avtalsvillkor, bestämmelser eller andra tillämpliga avtal relaterade till ändringar av avtalet inom ramen för dessa klausuler, ska dessa klausuler ha företräde.

BILAGA XII

STANDARDAVTALSKLAUSULER

Definitioner

I standardavtalsklausulerna definieras de använda termerna enligt följande:

avtal: det skriftliga avtal som ingåtts mellan parterna avseende tillhandahållande av tjänster, eventuella ändringar eller tillägg till detta, samt alla handlingar som rör fullgörandet av avtalet/avtalen, inklusive i synnerhet dess tillägg.

tillägg: ett tillägg, schema eller underlag som uttryckligen hänvisas till i avtalet.

kund till databehandlingstjänster (kund): enligt definitionen i artikel 2.30 i dataförordningen en fysisk eller juridisk person som har ingått ett avtalsförhållande med en leverantör av databehandlingstjänster i syfte att använda en eller flera databehandlingstjänster.

data: enligt definitionen i artikel 2.1 i dataförordningen varje digital återgivning av handlingar, fakta eller information och varje sammanställning av sådana handlingar, fakta eller information, även i form av ljudupptagningar, bildupptagningar eller audiovisuella upptagningar.

dataförordningen: förordning (EU) 2023/2854.

uttagsavgifter för data: enligt definitionen i artikel 2.35 i dataförordningen avgifter för dataöverföring som tas ut av kunder för att de ska kunna extrahera sina data genom nätverket från IKT-infrastrukturen hos en leverantör av databehandlingstjänster till en annan leverantörs system eller till lokal IKT-infrastruktur.

databehandlingstjänst: enligt definitionen i artikel 2.8 i dataförordningen en digital tjänst som tillhandahålls en kund och som möjliggör allmän nätverkstillgång på begäran till en gemensam pool av konfigurerbara, skalbara och elastiska databehandlingsresurser av centraliserad, distribuerad eller mycket distribuerad art och som snabbt kan tillhandahållas och levereras med minsta möjliga administration eller interaktion med tjänsteleverantören. I detta avtal avses med nämnda databehandlingstjänster de tjänster som leverantören tillhandahåller eller ska tillhandahålla kunden enligt avtalet.

destinationsleverantör: som nämns i artikel 2.34 i dataförordningen, den leverantör av databehandlingstjänster som kunden till en databehandlingstjänst byter till för att använda en annan databehandlingstjänst av samma tjänstetyp eller andra tjänster.

ursprunglig leverantör: som nämns i artikel 2.34 i dataförordningen, den juridiska person med vilken kunden har ingått ett avtalsförhållande avseende tillhandahållande av databehandlingstjänster och andra tjänster av leverantören enligt avtalet, och från vilken kunden nu avser att byta till en annan leverantör.

digitala tillgångar: enligt definitionen i artikel 2.32 i dataförordningen element i digitalt format, inbegripet applikationer, för vilka kunden har nyttjanderätt, oberoende av avtalsförhållandet med den databehandlingstjänst som kunden avser att byta från.

exporterbara data: enligt definitionen i artikel 2.38 i dataförordningen in- och utdata, inklusive metadata, som direkt eller indirekt genereras eller samgenereras genom kundens användning av databehandlingstjänsten, med undantag för tillgångar eller data som skyddas genom immateriella rättigheter, eller som utgör en företagshemlighet, som tillhör leverantörer av databehandlingstjänster eller tredje parter.

incident: en fysisk, teknisk eller organisatorisk säkerhetsöverträdelse, incident eller liknande händelse som kan ha en betydande inverkan på säkerheten och driftskontinuiteten, eftersom den har orsakat eller kan orsaka allvarliga störningar i tillämpliga it-system och verksamheter som används mellan leverantören och kunden under bytet, eller med avseende på kundens användning av tjänsterna, kundens exporterbara data och digitala tillgångar. Se standardavtalsklausulerna om säkerhet och driftskontinuitet.

interoperabilitet: enligt definitionen i artikel 2.40 i dataförordningen förmågan hos två eller flera dataområden eller kommunikationsnät, system, uppkopplade produkter, applikationer, databehandlingstjänster eller komponenter att utbyta och använda data för att utföra sina funktioner.

metadata: enligt definitionen i artikel 2.2 i dataförordningen en strukturerad beskrivning av innehållet i eller användningen av data som underlättar sökningen i eller användningen av dessa data.

icke-personuppgifter: enligt definitionen i artikel 2.4 i dataförordningen andra data än personuppgifter.

lokal IKT-infrastruktur: enligt definitionen i artikel 2.33 i dataförordningen IKT-infrastruktur och databehandlingsresurser som ägs, hyrs eller leasas av kunden, är belägna i kundens egen datacentral och drivs av kunden eller en tredje part.

övriga tjänster: alla professionella tjänster av vilket slag som helst som leverantören tillhandahåller kunden enligt avtalet, såsom det definieras däri, och som inte är databehandlingstjänster.

part: antingen kunden eller leverantören.

parter: både kunden och leverantören.

personuppgifter: enligt definitionen i artikel 4.1 i förordning (EU) 2016/679 (allmänna dataskyddsförordningen).

plan: den bytes- och utträdesplan som avses i standardavtalsklausulerna om byte och utträde, alternativ A, enligt överenskommelse mellan parterna enligt avtalet.

behandling: enligt definitionen i artikel 2.7 i dataförordningen en åtgärd eller kombination av åtgärder som utförs på data eller datamängder, oberoende av om de utförs automatiserat eller inte, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämnande genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

leverantör av databehandlingstjänster (leverantör): en fysisk eller juridisk person som har ingått ett avtalsförhållande med en kund i syfte att tillhandahålla en eller flera databehandlingstjänster.

samma tjänstetyp: enligt definitionen i artikel 2.9 i dataförordningen en uppsättning databehandlingstjänster som delar samma primära mål, databehandlingstjänstemodell och huvudsakliga funktioner.

tjänster: både databehandlingstjänsterna och alla andra tjänster som parterna har kommit överens om i avtalet.

tjänsteavgift: de avgifter som kunden är skyldig leverantören som ersättning för tillhandahållandet av tjänster enligt parternas överenskommelse i avtalet.

byte: enligt definitionen i artikel 2.34 i dataförordningen process som inbegriper en ursprunglig leverantör av databehandlingstjänster, en kund till en databehandlingstjänst och, i tillämpliga fall, en destinationsleverantör av databehandlingstjänster, varigenom kunden till en databehandlingstjänst byter från användning av en databehandlingstjänst till användning av en annan databehandlingstjänst av samma tjänstetyp eller en annan tjänst som erbjuds av en annan leverantör av databehandlingstjänster, eller till lokal IKT-infrastruktur, inbegripet genom extrahering, anpassning och uppladdning av data.

bytesavgifter: enligt definitionen i artikel 2.36 i dataförordningen andra avgifter än standardavgifter eller straffavgifter för förtida uppsägning som en leverantör av databehandlingstjänster tar ut av en kund för de åtgärder som föreskrivs i dataförordningen för att byta till en annan leverantörs system eller till lokal IKT-infrastruktur, inbegripet uttagsavgifter för data.