

# Bindande företagsbestämmelser och rättigheter

---

## 1 Meddelandetext om bindande företagsbestämmelser och rättigheter

---

### 1.1 Översikt

Information om hur HPE behandlar Personuppgifter beskrivs i [HPE Privacy Statement](#) (HPE dataskyddspolicy) eller i andra meddelanden som tillhandahålls vid tiden för insamling eller anställningsstart (för anställda). Detta meddelande innehåller ytterligare information om åtaganden från HPE:s sida med hänsyn till överföring av individers Personuppgifter och rättigheter under HPE:s bindande företagsbestämmelser.

### 1.2 Vad är HPE:s bindande företagsbestämmelser (Binding Corporate Rules - BCRs)?

HPE:s bindande företagsbestämmelser för Personuppgiftsansvariga (BCR-C) och bindande företagsbestämmelser för Personuppgiftsbiträden (BCR-P) är ramverk för företagets integritetsfrågor, vilka tillåter internationella överföringar av Personuppgifter utanför EES (Europeiska ekonomiska samarbetsområdet) och Schweiz i enlighet med europeisk dataskyddslagstiftning. De bindande företagsbestämmelserna innehåller ett bindande avtal undertecknat av [HPE-gruppen](#) tillsammans med affärsprocesser, policyer (inklusive [Global Master Privacy Policy](#), den globala integritetspolicyen), riktlinjer och utbildning. Alla anställda inom HPE-gruppen är bundna av de bindande företagsbestämmelser genom sina anställningsavtal, intern uppförandekod och olika HPE-policyer, standarder och specifikationer som tillämpas på bearbetningen av Personuppgifter.

Där lokal lagstiftning kräver en högre standard för dataskydd än de bindande företagsbestämmelserna, kommer den lokala lagstiftningen att ha företräde framför de bindande företagsbestämmelserna.

HPE-företag behandlar EU-registrerades Personuppgifter (såsom våra möjliga, nuvarande och tidigare anställda, villkorsanställda, leverantörer, kunder och affärskontakter) för att hantera vår arbetskraft, affärsverksamhet och affärsförbindelser. HPE-företag är Personuppgiftsansvariga för dessa Personuppgifter och avgör varför och hur Personuppgifter används. HPE:s BCR-C gör det möjligt för oss att överföra dessa Personuppgifter internationellt till andra medlemmar i vår världsomspännande grupp i enlighet med dataskyddslagstiftning i Europa, EES, Schweiz och Storbritannien.

HPE-företag behandlar även EU-registrerades Personuppgifter när vi tillhandahåller tjänster till våra Företagskunder. I detta fall är Företagskunden Personuppgiftsansvarig och HPE är Personuppgiftsbiträde eftersom vi behandlar Personuppgifter å Företagskundens vägnar och i enlighet med deras instruktioner. För vissa tjänster kan HPE:s BCR-P utnyttjas av våra Företagskunder för säkerställa att all överföring och behandling av deras Personuppgifter av HPE-gruppen i världen är förenlig med den europeiska dataskyddslagstiftningen (under förutsättning att detta ingår i avtalet mellan HPE och Företagskunden). Dessa åtaganden

innefattar en skyldighet för HPE-koncernen att samarbeta med våra Företagskunder, informera dem om en eventuell Personuppgiftsincident eller om HPE inte kan uppfylla BCR-P och hjälpa dem att uppfylla sina skyldigheter enligt den europeiska dataskyddslagstiftningen. BCR-P hjälper även våra Företagskunder att säkerställa att de kan ge respons när du utövar dina rättigheter i förhållande till dina Personuppgifter enligt tillämplig dataskyddslagstiftning.

Dessa ramverk för regelefterlevnad har godkänts av EU:s relevanta tillsynsmyndigheter och implementeras och förvaltas av HPE i samarbete med dessa tillsynsmyndigheter. Du kan genomdriva vissa rättigheter enligt de bindande företagsbestämmelserna. Mer information om dessa rättigheter och hur du utövar dem finner du nedan.

Definitionerna av termerna som används i detta meddelande beskrivs i slutet av dokumentet och kan nås [här](#).

*Om du önskar ytterligare information om våra bindande företagsbestämmelser, inklusive kopior av den relevanta texten i de kompletta reglerna eller detaljer om HPE-enheternas juridiska åtaganden enligt de bindande företagsbestämmelserna, eller önskar utöva dina rättigheter, kontakta HPE:s dataskyddsenhet genom att använda länken nedan.*

[Kontakta oss](#)

## 1.3 HPE:s åtaganden

### 1.3.1 HPE:s dataskyddsenhet

Dataskyddsenheten övervakar vårt integritetsskyddsprogram. Dataskyddsenheten ansvarar för att följa HPE:s sekretesspolicyer, inklusive de bindande företagsbestämmelserna. Dataskyddsenheten är behörig att undersöka eventuella misslyckanden från ett HPE-företags sida att följa de bindande företagsbestämmelserna och samråder med EU:s relevanta tillsynsmyndighet för att besluta om lämpliga åtgärder, om så är nödvändigt eller lämpligt.

Varje HPE-företag måste följa alla beslut som utfärdats av HPE:s dataskyddsenhet om de finns inte uppfylla de bindande företagsbestämmelserna.

### 1.3.2 Utbildning

Varje HPE-företag måste genomföra lämplig dataskydds - och säkerhetsutbildning som emellanåt utvecklas av dataskyddsenheten och HPE:s cybersäkerhets-team.

### 1.3.3 Samarbete

Alla HPE-företag måste samarbeta med alla EU-registrerade, Företagskunder och lämplig tillsynsmyndighet inom EU för att verifiera HPE-gruppens efterlevnad av de bindande företagsbestämmelserna, svara på eventuella frågor eller ge respons på eventuella klagomål som rör behandlingen av Personuppgifter i enlighet med de bindande företagsbestämmelserna.

### 1.3.4 Säkerhet och meddelanden om Personuppgiftsincident

Alla HPE-företag som behandlar EU-Personuppgifter måste genomföra lämpliga tekniska och organisatoriska åtgärder för att skydda sådana Personuppgifter mot Personuppgiftsincidenter. HPE-företaget måste också ta hänsyn till tillämplig dataskyddslagstiftning som gäller för dess Företagskunder och eventuella åtgärder som anges i Tjänsteavtalet med dessa Företagskunder.

Om en Personuppgiftsincident äger rum måste det relevanta HPE-företaget följa HPE:s säkerhetshanteringsprocess. När det gäller Personuppgifter tillhörande Registrerade inom EU gäller krav att HPE-företag:

- (i) dokumenterar Personuppgiftsincidenter;
- (ii) i fall där HPE-företaget är Personuppgiftsansvarig, meddelar berörda Registrerade om Personuppgiftsincidenten sannolikt kommer att medföra en hög risk för de Registrerade;
- (iii) i fall där HPE-företaget är Personuppgiftsansvarig rapporterar Personuppgiftsincidenten till relevant tillsynsmyndighet, biträdd av dataskyddsenheten där så krävs och
- (iv) i fall där Företagskunden är Personuppgiftsansvarig och HPE är Personuppgiftsbiträde, informerar HPE-företaget Företagskunden utan onödigt dröjsmål istället för att informera registrerade och EU:s tillsynsmyndigheter;

allt på ett sätt som uppfyller tillämplig dataskyddslagstiftning.

När HPE-företag agerar som Personuppgiftsbiträde ska HPE-företag hjälpa Företagskunderna att uppfylla sina skyldigheter med avseende på säkerhet, inbyggd

dataskydd och dataskydd som standard, Personuppgiftsincidenter och konsekvensbedömningar avseende dataskydd (enligt vad som anges i tillämplig dataskyddslagstiftning) med hänsyn till typen av behandling och den information som är tillgänglig för det relevanta HPE-företaget.

### 1.3.5 Sekretessprinciper

Alla HPE-företag följer europeiska dataskyddsprinciper både när vi agerar som Personuppgiftsansvarig och som Personuppgiftsbiträde.. Dessa principer beskrivs i [Global Master Privacy Policy](#), vår globala integritetspolicy.

Som Personuppgiftsansvarig:

- HPE-företag kan lämna ut dina Personuppgifter till tredje part, till exempel tjänsteleverantörer och leverantörer som stöder tillhandahållandet av våra tjänster inom kundsupport och marknadsföring samt företag som hanterar förmånsprogram för anställda. Mer information om vilka HPE-företag delar dina Personuppgifter med finns i vår integritetspolicy på nätet eller i andra meddelanden som lämnas vid insamlingstillfället eller vid anställningsstart (för anställda).
- Leverantörer och tjänsteleverantörer är skyldiga enligt avtal att hålla konfidentiell och säkra den information som de behandlar å HPE:s vägnar och får inte använda informationen till andra syften än att utföra tjänster för HPE:s räkning.
- Ett HPE-företag ska endast engagera ett Personuppgiftsbiträde för att behandla EU-Personuppgifter om Personuppgiftsbiträdet (i) får göra det enligt tillämplig HPE-policy och (ii) säkerställer att det finns ett skriftligt avtal som erkänns som giltigt enligt tillämplig dataskyddslagstiftning och som innehåller de föreskrivna bestämmelserna som anges i artikel 28, GDPR.
- När tredje parter finns i vissa länder utanför EES, Schweiz (eller Storbritannien, när Storbritannien har lämnat EU) som inte är länder som av EU-kommissionen bedömts erbjuda en adekvat skyddsnivå enligt tillämplig dataskyddslagstiftning, kommer HPE-företag att säkerställa att EU-Personuppgifter endast överförs i enlighet med tillämplig dataskyddslagstiftning och skyddas på ett adekvat sätt genom lämpliga skyddsåtgärder, såsom användning av kommissionens godkända standardavtalsklausuler eller annan åtgärd eller undantag som är relevant för det specifika fallet.

Som Personuppgiftsbiträde ska HPE-företag hjälpa den aktuella Företagskunden att uppfylla tillämpliga europeiska dataskyddsprinciper.

Som Personuppgiftsbiträde ska HPE-företag också säkerställa följande med avseende på relevanta sekretessprinciper:

## Ändamålsbegränsning

- Det måste finnas ett Tjänsteavtal med Företagskunden som omfattar behandling av EU-Personuppgifter.
- HPE-företag får endast behandla EU-Personuppgifter i syfte att leverera HPE-tjänster och i enlighet med:
  - Villkor för det relevanta Tjänsteavtalet, inklusive de som rör säkerhet och sekretess
  - Alla andra dokumenterade instruktioner för behandling som tillhandahålls av Företagskunden
  - HPE:s alla tillämpliga integritetspolicyer och andra tillämpliga policyer, standarder och förfaranden som ingår i BCR-P och
  - Alla tillämpliga lokala dataskydds- och integritetslagar. Om lokal lagstiftning kräver ett högre uppgiftsskydd än BCR-P, har den lokala lagstiftningen företräde framför de bindande företagsbestämmelserna.
- Om ett HPE-företag av någon anledning inte kan uppfylla villkoren för behandling (inklusive lagliga krav som påverkar dess skyldigheter i samband med Tjänsteavtalet), kommer HPE:s dataskyddsenhet, Hewlett-Packard The Hague B.V., Företagskunden och, i förekommande fall, Företagskundens behöriga EU-tillsynsmyndighet samt CNIL (Commission Nationale de l'Informatique et des Libertés, franska dataskyddsmyndigheten) att informeras.

## Radering eller förstörelse av Personuppgifter vid avslutning

- Vid avslutande av behandlingen av EU-Personuppgifter eller upphörande av Tjänsteavtalet kommer HPE-företag att följa instruktioner från Företagskunden för att returnera, radera eller förstöra alla kopior av sådana Personuppgifter och intyga att detta har gjorts.
- Om ett HPE-företag enligt lag är skyldigt att lagra Personuppgifter tillhörande EU-registrerade måste företaget sekretessbelägga Personuppgifterna och införa lämpliga säkerhetsåtgärder för att skydda Personuppgifterna.

## Datakvalitet

- HPE-företag ska uppdatera, korrigera eller ta bort EU-Personuppgifter i enlighet med Företagskundens instruktioner i den utsträckning som Företagskunden själv inte har tillgång till relevanta Personuppgifter. I förekommande fall, med hänsyn till typen av behandling, ska de informera andra HPE-företag eller tredje part till vilka sådana Personuppgifter har meddelats, att detta gjorts. Om så önskas av Företagskunden och i den utsträckning som det rimligen är möjligt och inom rimlig tid, kommer HPE-företagen att vidta åtgärder för att radera eller anonymisera EU-Personuppgifter. Detta sker när kunden fastställer att identifiering av sådana Personuppgifter inte längre är nödvändigt och, om tillämpligt, med hänsyn till typen av behandling, informera andra HPE-företag eller tredje part till vilka sådana Personuppgifter har lämnats, att detta gjorts.

## Lagring av uppgifter

- HPE-företag ska behålla EU-Personuppgifter under Tjänsteavtalets löptid med Företagskunden om inte annat anges av Företagskunden eller genom annan skriftlig instruktion.

## Ansvarsskyldighet

- För att visa efterlevnad av BCR-P och tillämplig dataskyddslagstiftning måste HPE-företag (i) upprätta en förteckning över sin behandling av EU-Personuppgifter som kan ställas till en EU-tillsynsmyndighets förfogande på begäran och (ii) utse ett dataskyddsombud, om GDPR gäller och kräver detta.

## Uppgiftsbehandling av Underbiträde

- **Uppgiftsbehandling av Underbiträde inom HPE-gruppen**

HPE-företag ska inte överföra eller tillåta att ett annat HPE-företag har tillgång till eller behandlar EU-Personuppgifter såvida inte bolaget har undertecknat BCR-P och har Företagskundens medgivande.

- **Uppgiftsbehandling av Underbiträde utanför HPE-gruppen**

HPE-företag kommer inte att överföra EU-Personuppgifter till ett externt Underbiträde såvida det inte har Företagskundens medgivande. Det kommer också att finnas ett skriftligt avtal med Underbiträdet som innehåller skyldigheter som väsentligen liknar de relevanta skyldigheterna i Tjänsteavtalet, vissa krav från BCR-P samt säkerställer ett adekvat skydd av alla EU-Personuppgifter som överförs internationellt i enlighet med tillämplig dataskyddslagstiftning.

- **Utse ersättare för Underbiträden**

Om ett HPE-företag utser en ny HPE- eller externt Underbiträde, kommer Företagskunden att meddelas och ha tio arbetsdagar på sig att motsätta sig denna förändring. Om Företagskundens invändning inte kan lösas kan företaget antingen avbryta överföringen eller behandlingen eller avsluta Tjänsteavtalet.

- **Ansvar för handlingar och försummelser från underbitrådets sida**

HPE-företagen förblir ansvariga för alla handlingar och försummelser av Underbiträdet som leder till en överträdelse av BCR-P.

### 1.3.6 Uppfyllande av EU-registrerades rättigheter

Som Personuppgiftsansvariga måste HPE-företagen uppfylla giltiga krav från EU-registrerade att utöva sina rättigheter att få tillgång till eller överföra sina Personuppgifter, att korrigera dem, att radera eller begränsa behandlingen av sina Personuppgifter och att invända mot viss behandling av sina Personuppgifter. Alla HPE-företag måste också se till att det inte fattar något beslut uteslutande baserat på automatiserad behandling av EU-registrerades Personuppgifter, inklusive profilering som ger rättsverkningar eller har liknande signifikanta rättsverkningar, om detta inte tillåts av och är i linje med de garantier som krävs av tillämplig dataskyddslagstiftning och efter samråd med dataskyddsenheten.

Om ett HPE-företag fungerar som Personuppgiftsbiträde, kommer det att meddela Företagskunden om det mottar en begäran från en EU-registrerad och kommer att samarbeta och tillhandahålla hjälp till företaget så att de kan uppfylla sina skyldigheter enligt tillämplig dataskyddslagstiftning.

## 1.4 Klagomålshantering och verkställighet av bindande företagsbestämmelser

Detta avsnitt beskriver hur du kan anföra klagomål till HPE och de förfaranden vi följer för att hantera ditt klagomål.

HPE-gruppen har genomfört ett klagomåls- och förlikningsförfarande som syftar till att tillämpa konsekventa incidenthanteringsprocedurer från identifiering till lösning. HPE:s dataskyddsenhet ansvarar för hanteringen av klagomål.

- Om du är EU-registrerad och tror att ett HPE-företag behandlar dina Personuppgifter som Personuppgiftsbiträde rekommenderar vi starkt att du först kontaktar den relevanta Personuppgiftsansvariga (vanligtvis Företagskunden). Om vi mottar ett klagomål från dig, är vi skyldiga enligt våra avtal och bindande företagsbestämmelser att vidarebefordra det till den relevanta Företagskunden (eller Personuppgiftsansvarig) om Företagskunden (eller Personuppgiftsansvarig) inte ber HPE att hantera det eller om de inte längre existerar. I det fallet kommer HPE:s dataskyddsenhet att samarbeta med Hewlett-Packard the Hague B.V. för att lösa klagomålet.
- Om du är EU-registrerad och har skäl att tro att ett HPE-företag inte har följt de bindande företagsbestämmelserna, kan du anföra klagomål direkt mot HPE-gruppen.
- Om du vill anföra klagomål direkt mot HPE-gruppen ska du kontakta HPE:s dataskyddsenhet via formuläret [Återkopplingsblankett sekretess](#) och antingen skicka in ditt klagomål eller begära att HPE:s dataskyddsenhet kontaktar dig via telefon. HPE:s dataskyddsenhet måste följa upp med det HPE-företag som är uppgiftsutförare (eller Hewlett Packard the Hague B.V., med avseende på BCR-P) i syfte att lösa klagomålet utan onödigt dröjsmål och under alla omständigheter inom en månad efter mottagandet (som kan förlängas med två månader om begäran är komplex och omfattar ett stort antal, i vilket fall den EU-registrerade måste informeras om förlängningen). Eventuella klagomål kommer att undersökas av en person med lämplig nivå av opartiskhet.
- Om klagomålet bedöms vara motiverat måste de relevanta HPE-företagen vidta de lämpliga korrigerande åtgärder som är nödvändiga för att lösa klagomålet och säkerställa att de bindande företagsbestämmelserna följs.
- Du kan också anföra klagomål hos EU:s tillsynsmyndighet i det land där du bor eller arbetar eller där den påstådda överträdelsen ägde rum eller vid domstolarna i det land där du bor eller där den ursprungliga uppgiftsutföraren är etablerad (eller i fallet med BCR-P vid domstolarna i Nederländerna där Hewlett Packard the Hague B.V. är etablerad). Du är fri att göra detta oavsett om du först har anfört ett klagomål mot oss eller inte.
- När vi agerar som Personuppgiftsbiträde har Företagskunder som tror att våra bindande företagsbestämmelser inte har följts rätt att begära rättslig prövning eller kräva ersättning från oss, inklusive för överträdelse av bindande företagsbestämmelser som orsakats av interna eller externa Underbiträden.

*Om du vill ha mer information om våra bindande företagsbestämmelser, inklusive kopior av den fullständiga texten till reglerna eller detaljer om de juridiska åtagandena hos HPE-enheter enligt de bindande företagsbestämmelserna eller önskar utöva dina rättigheter, kontakta HPE:s dataskyddsenhet med hjälp av [Återkopplingsblankett sekretess](#).*

## 1.5 Ansvar

Varje HPE-företag ansvarar för att följa de bindande företagsbestämmelserna.

Om du anför klagomål om att du lidit skada (inklusive ekonomisk och icke-materiell skada), så kommer den ursprungliga uppgiftsutföraren (i fallet med BCR-C) eller Hewlett Packard The Hague B.V. (i fallet med BCR-P) att:

- (i) vara ansvarig gentemot dig för de eventuella skador som du lidit till följd av överträdelsen som om det uppstått av eget förorsakande eller av egen underlåtenhet
- (ii) vidta nödvändiga åtgärder för att avhjälpa överträdelsen och
- (iii) kompensera dig för eventuella skador som uppkommit som en direkt följd av överträdelsen.

om vi inte kan visa att HPE-uppgiftsinförare och externa Underbiträden inte är ansvariga för händelsen som orsakat skadan.

Dessutom, om du har försökt att vidta åtgärder mot Företagskunden (som Personuppgiftsansvarig) och misslyckades eftersom

- (i) den faktiskt har försvunnit eller upphört att existera i lag eller har blivit insolvent och
- (ii) du kan visa att du har lidit skada och kan fastställa fakta som visar att det är troligt att detta beror på den relevanta överträdelsen

kommer Hewlett Packard the Hague B.V. också att kompensera dig om det inte kan visa att det tillämpliga HPE-företaget inte är ansvarigt.

Observera att du har dessa rättigheter utöver dina rättigheter enligt nationell dataskyddslagstiftning att anför ett klagomål mot din lokala EU-tillsynsmyndighet eller begära rättslig prövning i din lokala domstol, vilket kan innefatta att anför ett klagomål mot Hewlett Packard the Hague BV för hela skadan.

## 1.6 Lagval

I fall där lokala lagar kan hindra ett HPE-företag från att uppfylla sina skyldigheter enligt bindande företagsbestämmelser eller har en väsentlig inverkan på de garantier de bindande företagsbestämmelserna tillhandahåller, kommer HPE:s dataskyddsenhet att rapportera ärendet till tillämplig EU-tillsynsmyndighet (om inte det är förbjudet enligt sekretesskrav) såsom krävs för att lösa ärendet i samarbete med lämpliga myndigheter. Detta inkluderar alla rättsligt bindande ansökningar av en brottsbekämpande myndighet eller statlig säkerhetsorganisation om utlämnande av Personuppgifter tillhörande en EU-registrerad.

Om HPE:s dataskyddsenhet är förhindrad från att göra det kommer den att försöka få rätt att upphäva sådant förbud och kunna ge så mycket information som möjligt till tillämplig EU-



tillsynsmyndighet och, om så begärs, tillhandahålla information för att visa vilka åtgärder den har vidtagit enligt detta avsnitt (om inte detta skulle vara förbjudet enligt sekretesskrav).

Om dataskyddsenheten inte har möjlighet att lagligen notifiera relevant EU-tillsynsmyndighet ska dataskyddsenheten årligen offentliggöra allmän information om de ansökningar som mottagits av HPE-företag.

Eventuella utlämnanden av uppgifter till brottsbekämpande myndigheter eller statliga säkerhetsorgan som svar på en begäran ska göras i enlighet med tillämplig dataskyddslagstiftning.

När ett HPE-företag agerar som Personuppgiftsbiträde och får en juridiskt bindande ansökan av en brottsbekämpande myndighet eller statliga säkerhetsorgan om utlämnande av Personuppgifter tillhörande en registrerad inom EU, måste HPE-företaget bedöma begäran och göra ett uppehåll i behandlingen under en rimlig tidsperiod så att den kan meddela EU:s relevanta tillsynsmyndighet och Företagskunden (om så inte är förbjudet, t.ex. enligt straffrätten).

Om HPE-företaget är förbjudet att göra detta kommer det att försöka få rätt att upphäva detta förbud och ge så mycket information som möjligt till Företagskunden och/eller den relevanta EU-tillsynsmyndigheten.

Om HPE-företaget inte har möjlighet att lagligen informera tillsynsmyndighet och Företagskund, ska HPE-företaget årligen publicera generell information om juridiskt bindande förfrågningar om Personuppgifter som mottagits av HPE.

\*\*\*\*\*

## 1.7 Huvuddefinitioner

Nedan följer en översikt över de viktigaste definitionerna av termer som används i detta meddelande och/eller i de bindande avtal som tecknas av gruppens företag som ingår i HPE:s BCR-C och BCR-P.

<b>Behandla eller behandling</b>	avser all hantering av Personuppgifter, oavsett om det sker automatiskt eller ej, såsom insamling, inspelning, organisation, lagring, anpassning eller ändring, hämtning, konsultation, användning, avslöjande genom överföring, spridning eller på annat sätt tillgängliggöra inriktning, kombination, begränsning, radering eller förstörelse;
<b>Personuppgiftsansvarig</b>	avser en enhet (vare sig en fysisk eller juridisk person, offentlig myndighet, byrå eller annat organ) som ensam eller gemensamt med andra bestämmer syftet med och sättet att Behandla Personuppgifter
<b>Kundens Personuppgifter</b>	avser alla Personuppgifter i relation till vilka (i) kunden är personuppgiftsansvarig eller (ii) kunden är personuppgiftsbiträde på uppdrag av en personuppgiftsansvarig som har auktoriserat utnämningen av något HPE-företag som underbiträde och som Behandlas av ett HPE-företag som personuppgiftsbiträde eller underbiträde i syfte att leverera en HPE-tjänst
<b>Företagskund</b>	avser HPE-gruppens Företagskunder. Med avseende på BCR-P är det vanligtvis företaget som samlar in Personuppgifter från dig.
<b>EU-registrerad</b>	innebär varje identifierbar fysisk person inom EU som berörs av EU:s dataskyddslagstiftning.
<b>Europeiska ekonomiska samarbetsområdet (eller EES)</b>	avser zonen för ekonomiskt samarbete känt som det Europeiska ekonomiska samarbetsområdet och de länder som tillsammans är deltagare i en sådan zon <sup>1</sup> .
<b>EU-Personuppgifter</b>	avser alla Personuppgifter som behandlas eller har behandlats av ett HPE-företag och där

<sup>1</sup> I september 2018 medlemsstaterna i EU (Belgien, Bulgarien, Cypern, Danmark, Estland, Finland, Frankrike, Grekland, Irland, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Nederländerna, Polen, Portugal, Rumänien, Slovakien, Slovenien, Spanien, Sverige, Storbritannien, Tjeckien, Tyskland, Ungern, Österrike) samt Island, Lichtenstein och Norge.

	GDPR eller annan dataskyddslagstiftning gällande i EES, Schweiz eller Storbritanniens (när Storbritannien upphör att vara en medlemsstat i EU) är tillämplig.
<b>EU-tillsynsmyndighet</b>	avser en myndighet med reglerande befogenheter med hänsyn till skyddet av Personuppgifter som fastställts av en medlemsstat under GDPR.
<b>GDPR</b>	avser General Data Protection Regulation 2016/679, den allmänna europeiska dataskyddsförordningen.
<b>HPE</b>	avser Hewlett Packard Enterprise Company, som har sitt huvudkontor i Santa Clara, Kalifornien, USA.
<b>HPE-företag</b>	avser en medlem av HPE-gruppen som omfattas av BCR-C eller BCR-P och som har undertecknat det koncerninterna avtalet som binder varje enhet att följa de bindande företagsbestämmelserna.
<b>HPE-uppgiftsinförare</b>	avser ett HPE-företag baserat i ett tredje land utanför EU, EES eller Schweiz och Storbritannien (när Storbritannien upphört att vara en medlemsstat i EU) som Behandlar EU-Personuppgifter som direkt mottagits från en kunduppgiftsutförare eller en HPE-personuppgiftbiträde och uppgiftsutförare eller ett annat HPE-företag
<b>HPE-gruppen</b>	avser HPE och alla dess majoritetsägda och -kontrollerade dotterbolag oberoende av registreringsland eller verksamhet. En lista finns tillgänglig på <a href="https://www.hpe.com/us/en/ww-office-locations.html">https://www.hpe.com/us/en/ww-office-locations.html</a>
<b>HPE:s Personuppgifter</b>	avser alla Personuppgifter för vilka ett HPE-företag är personuppgiftsansvarig.
<b>HPE:s dataskyddspolicyer</b>	avser alla HPE-policyer, operativa förfaranden, vägledning och personalutbildning i samband med dataskydd, integritet och säkerhet, oavsett om det utfärdats av HPE för att få övergripande effekt globalt samt godkänts och publicerat av HPE som en del av dess globala policy eller om det utfärdats av något HPE-företag för att uppfylla kraven i lokal lag eller i ett Tjänsteavtal.
<b>HPE-personuppgiftsbiträde och uppgiftsutförare</b>	avser ett HPE-företag i EU, EES eller Schweiz eller Storbritannien (när Storbritannien har upphört att vara EU-medlem) som samtycker till att överföra EU-Personuppgifter å kundens vägnar från EU, EES, Schweiz eller Storbritannien (när Storbritannien har upphört

	att vara en EU-medlemsstat) till ett tredje land utanför EU, EES Schweiz eller Storbritannien (när Storbritannien har upphört att vara en EU-medlemsstat)
<b>HPE-tjänster</b>	avser alla IT-produkter eller -tjänster som säljs av ett HPE-företag till en Företagskund.
<b>Personuppgifter</b>	avser all information som rör en identifierad eller identifierbar fysisk person. En identifierbar fysisk person är en som kan identifieras direkt eller indirekt, särskilt med hänvisning till en identifierare, såsom namn, identifikationsnummer, platsdata, nätidentifierare eller till en eller flera faktorer som är specifika för hans fysiska, fysiologiska, genetiska, mentala, ekonomiska, kulturella eller sociala identitet, inklusive känsliga Personuppgifter och annan information som anses vara Personuppgifter enligt tillämplig lag om dataskydd.
<b>Personuppgiftsincident</b>	avser en brist i säkerheten som leder till oavsiktlig eller olaglig förstörelse, förlust, ändring eller obehörigt avslöjande av eller tillgång till Personuppgifter.
<b>Behandla eller behandling</b>	avser all hantering av Personuppgifter, oavsett om det sker automatiskt eller ej, såsom insamling, inspelning, organisation, lagring, anpassning eller ändring, hämtning, konsultation, användning, avslöjande genom överföring, spridning eller på annat sätt tillgängliggöra inriktning, kombination, begränsning, radering eller förstörelse;
<b>Personuppgiftsbiträde</b>	avser en enhet (vare sig en fysisk eller juridisk person, offentlig myndighet, byrå eller något annat organ) som behandlar Personuppgifter på uppdrag av och efter personuppgiftsansvarigs instruktioner
<b>Tjänsteavtal</b>	avser ett skriftligt avtal mellan ett HPE-företag och en Företagskund för HPE:s tjänster, vilka tillämpar BCR-P för behandling och överföring av kundens Personuppgifter helt eller delvis i samband med tillhandahållandet av relevanta HPE-tjänster.
<b>Underbiträde</b>	avser ett HPE-företag som giltigt utsetts till personuppgiftsbiträde för kundens Personuppgifter.
<b>Externt underbiträde</b>	avser varje tredjepart som har fått i uppdrag av ett HPE-företag att bistå med leverans av HPE-tjänster och som kommer att behandla Personuppgifter.

