

Beskrivning av behandlingen av personuppgifter och instruktioner från den personuppgiftsansvarige

1. Parter

Personuppgiftsansvarig: Tillgänglighetsbiblioteket Celia

Personuppgiftsbiträde: Samarbetspartner enligt avtalet

2. Bilagans syfte

Den personuppgiftsansvarige har ingått ett Avtal med Personuppgiftsbiträdet avseende en tjänst där Personuppgiftsbiträdet agerar personuppgiftsbiträde för personuppgifter som ingår i det personregister som den Personuppgiftsansvarige ansvarar för. Detta dokument beskriver de behandlingsåtgärder som Personuppgiftsbiträdet i egenskap av Personuppgiftsbiträde utför för den Personuppgiftsansvariges räkning, vilka typer av personuppgifter och vilka personuppgifter som behandlas. De för Personuppgiftsbiträdet bindande tekniska och organisatoriska åtgärderna har beskrivits i den Personuppgiftsansvariges anvisningar.

3. Syfte med och karaktären på behandling av personuppgifter

Syftet med behandlingen av personuppgifter: registrering av nya privatkunder som Celias kunder i bibliotekssystemet, underhåll av uppgifter om privatkunder, assisterande av privatkunder vid användning av Celias tjänster och underhåll av Samarbetspartners anställdas inloggningskoder.

Rättslig grund för behandling av personuppgifter:

- EU:s allmänna dataskyddsförordning artikel 6.1 a: Den registrerade har lämnat sitt samtycke till att dennes personuppgifter behandlas för ett eller flera specifika ändamål.
- EU:s allmänna dataskyddsförordning artikel 6.1 b: Behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.

- Artikel 6.1 c i EU:s allmänna dataskyddsförordning: Fullgörande av en rättslig förpliktelse som åvilar den personuppgiftsansvarige.
- EU:s allmänna dataskyddsförordning artikel 9 (särskilda kategorier av personuppgifter)
2 b: Fullgörande av en rättslig förpliktelse som åvilar den personuppgiftsansvarige.

Behandlingen sker primärt på grundval av den Personuppgiftsansvariges lagstadgade uppgift. I andra hand är det möjligt att den registrerade ger sitt samtycke till behandlingen och att behandlingen av personuppgifter utförs medan samtycket är i kraft.

Personuppgiftsbiträdet erhåller inloggningsuppgifter till det system som administreras av Celia, där Personuppgiftsbiträdet kan sköta de uppgifter som anges i avtalet. Personuppgiftsbiträdet behandlar personuppgifterna i systemet endast när det finns orsak att utföra de uppgifter som överenskommits i avtalet. Även i detta fall behandlas personuppgifterna endast i den utsträckning det är nödvändigt.

4. Period för behandling av personuppgifter

Personuppgiftsbiträdet behandlar de personuppgifter som preciserats i denna bilaga så länge Avtalet är i kraft.

5. Typ av personuppgifter och kategorier av registrerade

De behandlade Personuppgifterna avser följande kategorier av registrerade:

- Privatkunder
- Arbetstagare

De behandlade personuppgifterna består av följande slag av personuppgifter:

- **Privatkundens uppgifter**, såsom namn, hemadress, telefonnummer, e-postadress, födelsedatum och läsnedsättning.
- **Arbetstagar- och personaluppgifter** såsom namn, användarnamn och e-postadress.

Särskilda kategorier av personuppgifter:

- Uppgifter om privatkundens hälsa, uppgifter om läsnedsättningen.

Beställaren definierar individens kundrelation i sig som en särskild kategori av personuppgifter och den är därmed konfidentiell.

6. Den personuppgiftsansvariges instruktioner

- Celias privatkunders uppgifter har definierats som känsliga uppgifter om särskilda kategorier av personuppgifter. Celia behandlar känsliga uppgifter om särskilda kategorier av personuppgifter enligt Artikel 9 för skötseln av Celias uppgift i enlighet med den nationella lagstiftningen (Lag om Tillgänglighetsbiblioteket Celia 787/2022). Dataskyddslagen föreskriver om åtgärder för skydd av särskilda kategorier av personuppgifter och därmed ska särskild försiktighet iakttagas vid behandlingen av känsliga uppgifter.
- Personuppgiftsbiträdet iakttar god databehandlingssed på det sätt som krävs enligt gällande dataskyddslagstiftning, god informationshanteringssed i enlighet med offentlighetslagen och informationshanteringslagen, bestämmelserna om skydd av personuppgifter och den Personuppgiftsansvariges anvisningar om behandling av data.
- Personuppgiftsbiträdet ska instruera och utbilda sin personal i nödvändig datasäkerhet och dataskyddspraxis i enlighet med vad som krävs enligt denna bilaga och lagstiftningen. Samma krav gäller för de anställda hos eventuella underleverantörer.
- Personuppgiftsbiträdet försäkrar sig om att de personer som är involverade i behandlingen av personuppgifter förbinder sig att följa den i Avtalet överenskomna tystnadsplikten eller att de omfattas av en lagstadgad tystnadsplikt. Samma krav gäller för de anställda hos eventuella underleverantörer.
- Personuppgiftsbiträdet ska underrätta den Personuppgiftsansvarige om ändringar i användarrättigheter som gäller Huvudanvändaren, om det sker förändringar i arbetsuppgifterna för Huvudanvändaren med avseende på användarrättigheterna.
- För att förhindra obehörig åtkomst till systemet och de konfidentiella uppgifterna i systemet ska Personuppgiftsbitrådets och dess underleverantörers lokaler vara på lämpligt sätt skyddade med lås och andra nödvändiga åtgärder.
- Personuppgiftsbiträdet ska underrätta den Personuppgiftsansvarige om en personuppgiftsincident samt andra väsentliga störningar eller problem i de tjänster som personuppgiftsbiträdet producerar och som kan påverka de Registrerades ställning och rättigheter. Anmälan ska göras utan onödigt dröjsmål efter det att Personuppgiftsbiträdet eller dennes underleverantör har fått kännedom om överträdelsen. Anmälan ska göras till Celias dataskyddsombud.

- Den Personuppgiftsansvarige och Personuppgiftsbiträdet kommer överens om överlåtelse av uppgifter till utomstående. Personuppgiftsbiträdet överlåter inte uppgifter utan skriftligt tillstånd av den Personuppgiftsansvarige.
- Personuppgiftsbiträdet är införstått med att Personuppgiftsbitrådets uppgifter lagras i systemet när det används.
- För att säkerställa att Personuppgiftsbiträdet följer avtalet och i synnerhet de tekniska och organisatoriska säkerhetsåtgärder som krävs för utförandet, har den Personuppgiftsansvarige eller en av denne befullmäktigad auditerare rätt att när som helst auditera eller granska den verksamhet som avtalats i Avtalet och dess bilagor.
- Den Personuppgiftsansvarige instruerar hur personuppgifter behandlas i informationssystemet. Mekanismen för beviljande av användarrättigheter till det system som tjänsten gäller är sådan att, i den utsträckning som Personuppgiftsbiträdet ansvarar för processen, skapar beviljandeprocessen ett spår där grunderna för beviljandet av åtkomsträttigheter till användaren kan ses.
- Personuppgiftsbiträdet ska använda personliga eller rollspecifika åtkomsträttigheter när hen skapar åtkomsträttigheter, från vilka den enskilda användarens åtkomsträttigheter kan fastställas.
- Personuppgiftsbiträdet säkerställer att de enheter, programvaror och system som Personuppgiftsbiträdet ansvarar för, gör tillräckliga loggar och verifieringskedjor över sin verksamhet och Personuppgiftsbiträdet förvarar loggarna över åtkomstkontroll relaterade till föremålet för tjänsten så att de inte kan ändras i efterhand. För att loggarna ska uppfylla tillräcklighetskraven, ska loggarna innehålla händelsens tidpunkt, den åtgärd som har vidtagits eller som man har försökt att vidta, upphovsman och dennes befogenheter, plats (t.ex. IP-adress) källan till ändringsinformationen samt information om åtgärdens resultat. Vid misslyckade fall ska orsaken (t.ex. användarrättighet saknas) registreras.
- Personuppgiftsbiträdet är skyldigt att iaktta särskild omsorg i fråga om sekretess, datasäkerhet och dataskydd. Utöver tystnadsplikten har personuppgifternas synlighet begränsats så mycket som möjligt och behandlingen av personuppgifter sker endast av motiverad anledning.

Med tekniska och organisatoriska åtgärder avses följande skyddsåtgärder som Personuppgiftsbiträdet aktivt ska vidta:

- Personalen har fått utbildning i enlighet med dataskyddet och skötseln av dataskyddsuppgifterna.
- Personalen har fått aktuella anvisningar och föreskrifter i anknytning till dataskydd och datasäkerhet.
- Personalen har tillräckliga sekretessavtal eller så omfattas de av lagstadgad tystnadsplikt.
- Personuppgiftsbitrådets lokaler är föremål för övervakning, vilket inkluderar teknisk övervakning av inomhusutrymmena eller en del av den via övervakningsutrustning (t.ex. kameraövervakning eller passerkontroll).
- Personuppgiftsbiträdet har en ändamålsenlig och tillräcklig process för intern åtkomstkontroll som beaktar behandlingens art avseende det informationssystem som tillhandahålls av den Personuppgiftsansvarige.
- Personuppgiftsbiträdet sörjer för datasäkerheten i informationssystemen i enlighet med gällande lagstiftning om behandling av personuppgifter och dataskydd.
- Om Personuppgiftsbiträdet behandlar uppgifter utanför det informationssystem som den Personuppgiftsansvarige tillhandahåller, ska uppgifterna krypteras.
- Om Personuppgiftsbiträdet behandlar personuppgifter utanför det informationssystem som den Personuppgiftsansvarige tillhandahåller, ska uppgifterna anonymiseras eller pseudonymiseras i mån av möjlighet.
- Personuppgiftsbiträdet genomför aktivt auditeringar av datasäkerheten och dataskyddet i de lokaler, den utrustning och de program där den Personuppgiftsansvariges uppgifter behandlas.
- Tillräcklig kryptering används vid Personuppgiftsbitrådets anslutningar för fjärråtkomst och inloggningen i det system som tillhandahålls av den Personuppgiftsansvarige sker med ur datasäkerhetsperspektiv lämpliga lösenord/auktoriseringsmekanismer.
- Personuppgiftsbiträdet använder kontroll- och övervakningslösningar (t.ex loggar, personliga användarnamn med starkt lösenord) i den utrustning där man loggar in i det system som tillhandahålls av den Personuppgiftsansvarige.
- Skyddet av uppgifter ska ombesörjas i alla behandlingsfaser, från insamlingen av uppgifterna till raderingen av uppgifterna. Säkerheten vid behandlingen förutsätter av den utrustning som används för att logga in i det system som den



Saavutettavuuskirjasto

CELIA

Personuppgiftsansvarige ansvarar för, exempelvis förmåga att garantera kontinuerlig konfidentialitet, integritet, tillgänglighet och feltolerans samt förmåga att snabbt återställa tillgången till uppgifter och åtkomsten till uppgifterna i händelse av ett fysiskt eller tekniskt fel.

