Revisionsnummer	Datum	Ersätter (annan revision och datum)
2018/1	2018-05-02	2017/1 (2017-12-18)

Utfärdare (namn)	Titel
Filip Anderson	GDPR information

02 maj 2018

Dataskydds-förordningen

GDPR

Innehållsförteckning

BAKGRUND 3

VAD ÄR DATASKYDDSFÖRORDNINGEN? 3
VAD ÄR NYTT? 3
MER INFORMATION 4

GDPR I PRAKTIKEN 4

PERSONUPPGIFTSANSVARIG OCH -BITRÄDE 4
BEHANDLING AV PERSONUPPGIFTER 4
DE REGISTRERADES RÄTTIGHETER 5
Rätt till information 5
Rätt till rättelse 5
Rätt till radering (”rätten att bli bortglömd”) 5
Rätt till begränsning av behandling 6
Dataportabilitet 6
Rätt att göra invändningar 6
Automatiserat beslutsfattande, inbegripet profilering 7
Klagomål 7
Skadestånd 7

SVAR PÅ VIKTIGA FRÅGOR 7

DATALAGRINGSPLATS 7
KRYPTERING 7
GALLRING 7
UNDERLEVERANTÖRER 8
KONTAKTPERSONER 8

Bakgrund

Vad är Dataskyddsförordningen?

EU har beslutat om en ny förordning som innehåller regler om hur man får behandla personuppgifter. Förordningen börjar gälla den 25 maj 2018 och kallas dataskyddsförordningen eller GDPR. Förordningen kommer att gälla direkt i alla EU:s medlemsländer och ersätter nationella regler som till exempel personuppgiftslagen i Sverige.

Mycket i dataskyddsförordningen liknar de regler som finns i personuppgiftslagen. På samma sätt som idag får man behandla personuppgifter med stöd av samtycke från de registrerade, för att uppfylla ett avtal eller efter en intresseavvägning till exempel. De registrerade kommer även i fortsättningen att ha rätt att få information om den personuppgiftsbehandling som sker - och den som behandlar personuppgifter måste ha tillräckliga säkerhetsåtgärder för att uppgifterna skyddas på rätt sätt. Om det är fråga om uppgifter om hälsa, etniskt ursprung, politisk uppfattning eller religiös tro ställs särskilda krav.

Vad är nytt?

- När uppgifter behandlas med stöd av samtycke eller för att uppfylla ett avtal, ska den registrerade ha rätt att få ut de uppgifter man själv lämnat för att föra över dem till en annan tjänst, det kallas **dataportabilitet**.
- Innan man planerar en ny personuppgiftsbehandling som innebär särskilda risker för de registrerade ska man göra en bedömning av vilka konsekvenser behandlingen kan få och vilka åtgärder som behövs för att minska riskerna (**konsekvensbedömning**).
- Om det inträffar en säkerhetsincident, till exempel ett dataintrång eller en oavsiktlig förlust av uppgifter, måste man anmäla det till Datainspektionen inom 72 timmar. Man kan också behöva informera de registrerade (**anmälan om personuppgiftsincident**).
- Vissa organisationer; myndigheter, de som behandlar känsliga uppgifter eller uppgifter som innebär en kartläggning av enskildas beteende måste utse en person i organisationen som har till särskild uppgift att bevaka dataskyddsfrågor, ett **dataskyddsombud**.
- Datainspektionen kan komma att utdöma en **sanktionsavgift** för den som bryter mot förordningens regler. Avgiften ska bedömas utifrån hur allvarlig överträdelsen är, om det skett avsiktligt eller inte, vilka åtgärder man har vidtagit för att minska skadan, om man tjänat ekonomiskt på överträdelsen och andra försvårande eller förmildrande omständigheter.
- I personuppgiftslagen finns en förenklad regel för behandling av personuppgifter i löpande text och enkla listor, **missbruksregeln**. Den innebär kort och gott att man får behandla uppgifter i vissa situationer så länge det inte är kränkande för någon. Den här regeln **försvinner** när dataskyddsförordningen träder ikraft. Sådan behandling måste alltså följa förordningens regler.

Mer information

Mer information om dataskyddsförordningen finns på Datainspektionens hemsida:
https://www.datainspektionen.se/dataskyddsreformen/

GDPR i praktiken

Personuppgiftsansvarig och -biträde

Som sagt så är GDPR väldigt likt PUL och många av de rutiner man har sedan tidigare behöver inte ändras, men det finns några saker som måste uppdateras.

Men först är det viktigt att förstå skillnaden mellan att vara Personuppgiftsansvarig och att vara Personuppgiftsbiträde.

Personuppgiftsansvarig är den organisation som äger personuppgifterna som finns i ett register. Om en tredje part används som mellanhand eller för att lagra personuppgifterna så räknas denna part som biträde.

Enligt detta så är ni som kund hos oss personuppgiftsansvariga, och vi agerar som personuppgiftsbiträde till er för att behandla ert data. Det innebär att vi enbart får behandla data i enlighet med ett personuppgiftbiträdesavtal och instruktioner som upprättas mellan oss. Det ligger med ett standardavtal för detta i våra kundavtal.

Mer information finns på Datainspektionens hemsida:
https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/skyldigheter-for-de-som-behandlar-personuppgifter/personuppgiftsansvarig/

https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/skyldigheter-for-de-som-behandlar-personuppgifter/personuppgiftsbitrade-och-bitradesavtal/

Behandling av personuppgifter

All behandling av personuppgifter måste uppfylla de grundläggande principer som anges i dataskyddsförordningen. Principerna innebär bland annat att personuppgifter bara får samlas in för berättigade ändamål som inte är alltför allmänt hållna och att mängden uppgifter ska begränsas till vad som är nödvändigt för ändamålen. Uppgifterna får inte senare behandlas på ett sätt som är oförenligt med dessa ändamål och inte heller sparas längre än nödvändigt. Den som behandlar personuppgifter ska kunna visa att principerna följs.

Mer information finns på Datainspektionens hemsida:
https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/principer-for-behandling-av-personuppgifter/

De registrerades rättigheter

De personer vars personuppgifter behandlas, de registrerade, har ett antal rättigheter enligt dataskyddsförordningen. Dessa rättigheter innebär i korthet att de registrerade ska få information om när och hur deras personuppgifter behandlas och ha kontroll över sina egna uppgifter. Därför har de bland annat rätt att i vissa fall få sina uppgifter rättade, raderade eller blockerade, eller att få ut eller flytta sina uppgifter. De registrerades rättigheter har utökats, förstärkts och specificerats i dataskyddsförordningen jämfört med personuppgiftslagen. Nedan följer en sammanfattning av rättigheterna och hur vi på Joliv kan hjälpa er att uppfylla dem.

Mer information finns på Datainspektionens hemsida:
https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/de-registrerades-rattigheter/

Rätt till information

Den registrerade har rätt att få information när hans eller hennes personuppgifter behandlas. Information om personuppgiftsbehandlingen ska lämnas av den personuppgiftsansvarige både när uppgifterna samlas in och när den registrerade annars begär det. Därutöver finns det vissa tillfällen när särskild information ska ges till den registrerade, till exempel om det inträffar ett dataintrång eller liknande (en personuppgiftsincident) hos den personuppgiftsansvarige och det finns risk för till exempel identitetsstöld eller bedrägeri.

Om någon av era registrerade begär ut sin information så har vi på Joliv rutiner för att ta fram detta åt er. I t.ex. mobilOMSORG finns en ny rapport som kan användas för att plocka fram ett datauttag. För andra produkter har vi manuella rutiner att ta fram detta på beställning från er.

Vi på Joliv har även rutiner för rapportering av incidenter till er. När ni får en incidentrapport från oss är det ert ansvar att vidare informera era kunder som är potentiellt drabbade.

Joliv skickar aldrig på egen hand ut information till någon av era registrerade.

Rätt till rättelse

Varje person har rätt att vända sig till ett företag eller myndighet som behandlar personuppgifter och be att få felaktiga uppgifter rättade. Det innebär också att den enskilde har rätt att komplettera med sådana personuppgifter som saknas och som är relevanta med hänsyn till ändamålet med personuppgiftsbehandlingen.

Rättning av personuppgifter kan i de flesta fall direkt göras av er i våra produkter. I undantagsfall så kan vi på Joliv hjälpa till om rättningen behöver göras med ett skript på en större mängd data.

Rätt till radering (”rätten att bli bortglömd”)

Varje person har rätt att vända sig till ett företag eller en myndighet som behandlar personuppgifter och be att uppgifterna som avser honom eller henne raderas.

I dessa fall behöver en bedömning göras om uppgifterna kan raderas. Det kan hända att de måste finnas kvar för att ni ska kunna fullgöra ett pågående avtal till den registrerade, eller för att andra lagkrav föreligger. Till exempel patientdatalagen.

Vi på Joliv kan bistå med radering enligt beställning från er, vi raderar inte data om en begäran inkommer direkt från någon av era registrerade.

Rätt till begränsning av behandling

Enskilda har i vissa fall rätt att kräva att behandlingen av personuppgifter begränsas. Med begränsning menas att uppgifterna markeras så att dessa i framtiden endast får behandlas för vissa avgränsade syften.

Detta är något som ni behöver ha koll på i er egen organisation. Våra produkter gör ingen skillnad på det data som behandlas då det är omöjligt att veta vad för sorts begränsningar som kan tänkas begäras.

Dataportabilitet

Den som har lämnat sina personuppgifter har i vissa fall rätt att få ut och använda sina personuppgifter på annat håll till exempel i en annan social medietjänst (rätten till dataportabilitet). Den som har tagit emot personuppgifterna är skyldig att underlätta en sådan överflyttning av personuppgifter. En förutsättning är att denna behandlar personuppgifterna med stöd av ett samtycke från den registrerade eller för att uppfylla ett avtal med den registrerade och det gäller bara sådana personuppgifter som den registrerade själv har lämnat.

Det finns inget standardiserat format för den typ av data som vi behandlar åt er, men det finns möjlighet att plocka ut relevant information i läsbart format som kan användas för att underlätta en flytt.

Rätt att göra invändningar

En enskild har i vissa fall rätt att invända mot den personuppgiftsansvariges behandling av hans eller hennes personuppgifter.

Rätten att invända gäller när personuppgifter behandlas för att utföra en uppgift av allmänt intresse, som ett led i myndighetsutövning eller efter en intresseavvägning.

Om den enskilde invänder mot behandlingen i sådana fall får den personuppgiftsansvarige endast fortsätta att behandla uppgifterna om det går att visa att det finns tvingande berättigade skäl till att uppgifterna måste behandlas som väger tyngre än den enskildes intressen, rättigheter och friheter eller om behandlingen sker för fastställande, utövande eller försvar av rättsliga anspråk.

Den enskilde har alltid rätt att invända mot att hans eller hennes personuppgifter används för direkt marknadsföring. En sådan invändning kan göras när som helst. Görs en invändning mot direkt marknadsföring, får personuppgifterna inte längre behandlas för sådana ändamål.

Detta är återigen något som ni själva behöver ha koll på i er organisation.

Automatiserat beslutsfattande, inbegripet profilering

Den enskilde har rätt att inte bli föremål för ett beslut som enbart grundas på någon form av automatiserat beslutsfattande, inbegripet profilering, om beslutet kan ha rättsliga följder för den enskilde eller på liknande sätt i betydande grad påverkar honom eller henne.

Automatiserat beslutsfattande kan till exempel vara ett automatiserat avslag på en kreditansökan på internet eller vid ett nekande besked från e-rekrytering via internet utan personlig kontakt.

Automatiserat beslutsfattande kan vara tillåtet om det är nödvändigt för ingående eller fullgörande av ett avtal mellan den registrerade och den personuppgiftsansvarige eller om den enskilde har gett sitt uttryckliga samtycke. Det kan även vara tillåtet enligt särskild lagstiftning.

Den autoplanering som görs i våra program räknas här in under det föregående stycket och är därmed tillåten.

Klagomål

Den som anser att någon behandlar uppgifter om honom eller henne i strid med dataskyddsförordningen kan lämna in ett klagomål till Datainspektionen. Datainspektionen tar del av alla klagomål och bedömer om tillsyn ska inledas och lämnar därefter besked till den som fört fram klagomålet.

Skadestånd

En person som har lidit skada på grund av att hans eller hennes personuppgifter har behandlats i strid med dataskyddsförordningen kan ha rätt till skadestånd av den eller de personuppgiftsansvariga som medverkat vid behandlingen.

Svar på viktiga frågor

Datalagringsplats

All data som behandlas av oss för er räkning lagras inom EU/EES.

Kryptering

Databasens lagringsmedia är krypterad och all data är krypterad vid överföring.

Gallring

Gallring sker på beställning från er organisation. Ni äger ert data och vi har ingen rätt att på eget bevåg utföra gallring.

Underleverantörer

Solid Park förvaltar våra servrar, vi har ett personuppgiftsbiträdesavtal med dem.

Kontaktpersoner

Ansvarig/Företrädare: Katarina Pihl, katarina.pihl@joliv.se

Dataskyddsombud: Filip Andersson, filip.andersson@joliv.se