www.pwc.se

Granskning av GDPR - Efterlevnad utifrån dataskyddsförordning-ens krav

Region Jönköpings Län

Rasmus Poulsen
Maricka Lundholm

Februari 2019

pwc

Innehåll

Sammanfattning

Bakgrund
GDPR trädde i kraft 25 maj 2018. PwC har på uppdrag av de förtroendevalda revisorerna i Region Jönköping genomfört en granskning av dataskyddsförordningens krav. Granskningen har omfattat intervjuer och dokumentstudier och genomförts under perioden oktober 18 – februari 19.

Revisionsfråga
Granskningen syftar till att bedöma om:

- Regionstyrelsen har vidtagit tillräckliga åtgärder för att säkerställa att Region Jönköping följer lagstiftningen enligt GDPR

Vi bedömer att regionstyrelsen delvis har vidtagit tillräckliga åtgärder för att säkerställa att Region Jönköping följer lagstiftningen enligt GDPR. Det finns en medvetenhet hos regionledningen samt dataskyddsombudet om kvarvarande arbete där man medvetet har skjutit på vissa delar då andra delar varit högre prioriterade.

Kontrollmål
Finns det ändamålsenliga policys, riktlinjer och instruktioner upprättade inom området?
Delvis uppfylld.

Finns registerförteckning upprättad för personuppgiftsbehandlingar inom styrelsens förvaltning/ar?
Uppfylld.

Har styrelsen genom beslut utsett ett dataskyddsombud?
Uppfylld.

Har styrelsen/nämnden genom beslut fastställt en ändamålsenlig arbetsbeskrivning för dataskyddsombudet utifrån dataskyddsförordningen krav?
Delvis uppfylld.

Har åtgärder vidtagits för att säkerställa att det hos medarbetarna inom förvaltningen/arna finns en tillräcklig kunskap om de krav som följer av dataskyddsförordningens ikraftträdande?
Delvis uppfylld.

Finns ett tillräckligt skydd för personuppgifterna, så att endast behöriga har tillgång till dem?
Delvis uppfylld.

Har organisationen system och rutiner för att proaktivt upptäcka förlust eller läckage av personuppgifter?
Delvis uppfylld.

Finns system och/eller rutiner för att hantera den registrerades rättigheter?
Delvis uppfylld.

Finns en ändamålsenlig organisation för incidenthantering utifrån dataskyddsförordningens krav?
Uppfylld.

Har konsekvensbedömningar gjorts på personuppgiftsbehandlingar som kan bedömas ha en påverkan på den registrerades rättigheter och friheter?
Ej uppfylld.

Rekommendationer

Mot bakgrund av vad som framkommit i granskningen ges följande rekommendationer:

- Fortsätt med transparens och öppna kommunikationsvägar för personal vad gäller dataskyddsfrågor.
- Ta fram en utbildningsplan framåt och utvärdera om uppföljning på om medarbetaren genomfört utbildning eller inte ska implementeras.
- Utvärdera förvaltningsgruppernas behov av resurser utifrån de uppgifter som de förväntas utföra.
- Säkerställ att dataskyddsombudet fortsättningsvis får samma goda förutsättningar att utföra sitt arbete som i dagsläget.
- Revidera och uppdatera behandlingsregistret, samt ta fram en förvaltningsprocess för att hålla behandlingsregistret aktuellt. Processen bör utgå från vad som ska göras om en ny behandling identifieras eller en befintlig behandling behöver ändras.
- Utvärdera samstämmigheten mellan de biträdesavtal som tecknats och de behandlingar som är upptagna i behandlingsregistret.
- För de rättigheter där process inte fastställts för förfrågan och hantering bör sådan fastställas, däribland rätten till radering och dataportabilitet.
- Ta fram en metod, process och rutin för att utföra konsekvensbedömningar (DPIA) på behandlingar som bedömts utgöra en hög risk.
- Gör en genomlysning och granskning av IT-säkerheten för att se om teknisk monitorering av avvikelser från dagligt arbete (BAU) bör prioriteras.
- Dokumentera de överväganden ni gjort om varför ni anser att ni når till en lämplig nivå av dataskydd för personuppgifter.
- Dokumentera en plan med prioritetsordning för kommande arbete avseende dataskydd.
- Dokumentera rollbeskrivning för dataskyddsombudet.

1. Inledning

1.1. Bakgrund

EU:s nya dataskyddsförordning General Data Protection Regulation, GDPR, innehåller regler om hur personuppgifter får behandlas. Förordningen började gälla den 25 maj 2018 och ersatte då personuppgiftslagen (PuL).

Förordningen innebär bland annat hårdare krav på hantering av personuppgifter. Vidare ställer förordningen krav på rutiner och processer för säker hantering av register. Detta medför även krav på ansvarig ledningsnivå att säkerställa efterlevnad av förordningen inom organisationen.

Nya dataskyddsförordningen gäller för alla organisationer och branscher som sparar eller på något sätt hanterar personlig och känslig information om sina anställda, leverantörer eller sina kunder.

Dataskyddsförordningen gäller för behandling av personuppgifter. Med personuppgifter avses varje upplysning som avser en identifierad eller identifierbar fysisk person. Avgörande är att uppgiften, enskilt eller i kombination med andra uppgifter, kan knytas till en levande person. Enklaste typen av personuppgifter är personnummer, namn och adress.

För att dataskyddsförordningen ska respekteras införs möjligheten till kraftfulla sanktioner för de organisationer som ignorerar eller brister i att uppfylla de nya kraven. Sanktionsnivåerna har valts så att de ska vara avskräckande och för att det inte ska löna sig att bryta mot reglerna för att spara pengar. De som inte följer förordningen riskerar bland annat sanktioner. Sanktionerna kan belasta organisationer som bryter mot lagkravet med viten på upp till 10 miljoner kronor för myndigheter beroende på överträdelsens art och omfattning. Det införs också en rätt för privatpersoner att kräva skadestånd av de organisationer som inte tillhandahåller deras rättigheter enligt förordningen.

Revisorerna i Region Jönköping har genom sin riskanalys för revisionsåret 2018 funnit det prioriterat att granska organisationens efterlevnad utifrån dataskyddsförordningens krav.

1.2. Syfte och Revisionsfråga

Granskningen syftar till att bedöma om:

- Regionstyrelsen har vidtagit tillräckliga åtgärder för att säkerställa att Region Jönköping följer lagstiftningen enligt GDPR

1.3. Avgränsning

Granskningen avgränsas till innehållet i lagstiftningen och good practice. Noterbart är att praxisfall ej kommer beröras då detta ännu inte finns i tillräckligt stor utsträckning för att kunna granska huruvida dessa är tillförlitliga.

Granskningen avgränsas till hur Regionstyrelsen har hanterat frågan om att implementera rutiner med anledning av GDPR. Granskningen kommer inte att omfatta detaljer i hur verksamheten har agerat.

1.4. Metod

Insamling och analys av, för området, relevanta styrdokument och stickprov.

Granskningen har genomförts genom intervjuer med regiondirektör, IT-direktör, kanslidirektör tillika informationssäkerhetsanvarig, informationssäkerhetschef samt dataskyddsombud. Intervjuer har även genomförts med ledningsfunktionen inom tre verksamhetsområden (Medicinsk vård, Vårdcentralerna Bra Liv och Verksamhetsstöd och service).

2. Iakttagelser och bedömningar

RJL:s regionledningskontor tillsatte en styrgrupp (ordf. kanslidirektör/informationssäkerhetsansvarig) och projektorganisation med en extern projektledare för arbetet med att implementera åtgärder för efterlevnad av GDPR. Utöver projektledaren tillsattes till en början fyra resurser (regionjurister, informationssäkerhetsspecialist, kommunikatör och dataskyddsombud) på mellan 25-50%. Projektet har sedan arbetat, med löpande rapportering till styrgruppen, med att ta fram och implementera åtgärder. De åtgärder man tagit fram har sedan skickats vidare till respektive verksamheter inom RJL där de själva fått anpassat sig.

Ett antal beslut och styrdokument för projektet har tagits fram av regionledningen:

- Programplan_GDPR_v1_1.docx
- Projektdirektiv_Tillampling_av_GDPR_v1_0.docx
- Projektplan_Tillampning_GDPR_v1_0.docx
- Projektdirektiv_Styrning_och_Ledning_GDPR_v1_0.docx
- Programdirektiv_GDPR_v1_3.docx
- Kommunikationsplan_GDPR_1_3.docx
- Projektplan_Ledning_och_StyrningGDPR_v1_0.docx

2.1. Finns det ändamålsenliga policys, riktlinjer och instruktioner upprättade inom området?

2.1.1. Iakttagelser

Externa riktlinjer i form av en integritetspolicy har sammanställts av RJL och publicerats på webbplatsen[1]. Denna innehåller relevanta delar inom GDPR, ex. den registrerades rättigheter, behandling och lagringstid samt rätten till att lämna klagomål.

Dokumentation (”Personuppgiftsbitradesavtal.docx”) och en mall för hur personuppgiftsbiträdesavtal ska upprättas (”MALL_Personuppgiftsbitradesavtal.docx”) har tagits fram och kan användas.

Ett antal interna riktlinjer och rutindokument finns framtagna för att stötta de anställda i sitt dagliga arbete:

- Konsekvensbedomning_och_forhandssamrad.docx
- Utbildningsmaterial_GDPR.pptx
- Riktlinje_Registerutdrag.docx
- Rutin_Registerutdrag___IT_kontaktpersoner.docx
- Register_over_personuppgiftsbehandlingar.docx
- Registerutdrag_mall.docx
- Rutin_personuppgiftsincident.docx
- Riktlinje___personuppgiftsincident.docx
- De_registrerades_rattigheter.docx
- MALL_Personuppgiftsbitradesavtal.docx
- Personuppgiftsbitradesavtal.docx
- Rutin_tillsynsmyndighet.docx
- Informationstextmall.docx
- Samtyckestext_mall.docx
- Riktlinje_hantering_av_personuppgifter_i_epost.docx
- Rutin_Registerutdrag_registrator.docx

[1] https://www.rjl.se/om-oss/kontakta-oss/persondataskydd-och-dataskyddsombud/

2.1.2. Bedömning

Kontrollmålet är delvis uppfyllt.

Som personuppgiftsansvarig har man så kallad ansvarsskyldighet. Detta innebär att man har en skyldighet att kunna visa att man efterlever dataskyddsförordningen. Om man inte har dokumenterat dataskyddsarbetet och de överväganden, analyser och beslut som tagits, innebär det en risk.

Vad vi ser finns grundläggande dokumentation på plats, dock har vi noterat att det finns beslut och processer som bör dokumenteras, t.ex varför RJL anser att de håller en lämplig nivå av dataskydd, rutiner för hantering av samtliga rättigheter samt process för konsekvensbedömning av dataskydd

Mot bakgrund av ovan anser vi att RJL delvis har uppfyllt kravet.

2.2. Finns registerförteckning upprättad för personuppgiftsbehandlingar inom styrelsens förvaltning/ar?

2.2.1. Iakttagelser

Varje verksamhetsansvarig inom RJL har haft ansvaret att se till att dess verksamhet har dokumenterat dess personuppgiftsbehandlingar. RJL har samlat in över 1000 personuppgiftsbehandlingar i ett register med hjälp av IT-systemet DraftIT. DraftIT ska enligt uppgift vara konfigurerat på ett sätt som endast gör det möjligt att registrera en behandling om samtliga nödvändiga fält är ifyllda.

I ett första steg har RJL samlat in data, inkl. ostrukturerade behandlingar, för att i ett senare steg komplettera, revidera och korrigera den data som insamlats.

I dagsläget har ingen uppföljning gjorts på om samtliga behandlingar har inkommit.

2.2.2. Bedömning

Kontrollmålet är uppfyllt.

Att upprätta ett personuppgiftsbehandlingsregister är en stor uppgift som tar lång tid. Det finns sannolikt flertalet identiska behandlingar, likväl som det sannolikt finns behandlingar med felaktigt tolkad laglig grund. RJL har tagit detta i beaktning och kommer därför att göra en genomgång och korrigering av det befintliga registret i framtiden. Tidpunkt för när detta ska göras är vad PwC förstår ännu inte fastställd.

Genom att samla in behandlingarna anser vi att RJL i nuläget har uppfyllt kravet på att upprätta en registerförteckning.

2.3. Har styrelsen genom beslut utsett ett dataskyddsombud?

2.3.1. Iakttagelser

Av våra intervjuer inom ramen för granskningen framgår att styrelsen och samtliga nämnder har genom beslut utsett ett dataskyddsombud. Vidare framgår att dataskyddsombudet är anmält till datainspektionen.

Dataskyddsombudet tillhör den juridiska verksamheten hos regionledningskontoret.

2.3.2. Bedömning

Kontrollmålet är uppfyllt.

Regionstyrelsen har beslutat, utsett och anmält ett dataskyddsombud till Datainspektionen. Vi anser därför att RJL har uppfyllt kravet.

2.4. Har styrelsen/nämnden genom beslut fastställt en ändamålsenlig arbetsbeskrivning för dataskyddsombudet utifrån dataskyddsförordningen krav?

2.4.1. Iakttagelser

Dataskyddsombudet ska enligt GDPR minst ha följande uppgifter:

a) Att informera och ge råd till den personuppgiftsansvarige eller personuppgiftsbiträdet och de anställda som behandlar om deras skyldigheter enligt GDPR och andra av unionens eller medlemsstaternas dataskyddsbestämmelser.

b) Att övervaka efterlevnaden av GDPR, av andra av unionens eller medlemsstaternas dataskyddsbestämmelser och av den personuppgiftsansvariges eller personuppgiftsbiträdets strategi för skydd av personuppgifter, inbegripet ansvarstilldelning, information till och utbildning av personal som deltar i behandling och tillhörande granskning.

c) Att på begäran ge råd vad gäller konsekvensbedömningen avseende dataskydd och övervaka genomförandet av den enligt artikel 35, GDPR.

d) Att samarbeta med tillsynsmyndigheten.

e) Att fungera som kontaktpunkt för tillsynsmyndigheten i frågor som rör behandling, inbegripet det förhandssamråd som avses i artikel 36, och vid behov samråda i alla andra frågor.

Dataskyddsombudet ska vid utförandet av sina uppgifter ta vederbörlig hänsyn till de risker som är förknippade med behandling, med beaktande av behandlingens art, omfattning, sammanhang och syften.

RJL har medvetet inte upprättat något explicit dokument med en arbetsbeskrivning för dataskyddsombudet. Det för att RJL vill analysera och identifiera vilka uppgifter som bör

ingå i dataskyddsombudets roll innan man upprättar en arbetsbeskrivning. PwC har inte tagit del av någon plan för när detta arbete ska ske.

RJL har upprättat ett antal riktlinjer och rutiner avseende GDPR (se 2.1.1). I dessa förklaras delvis dataskyddsombudets ansvar i enlighet med ovan punkter (a-e).

2.4.2. Bedömning

Kontrollmålet är delvis uppfyllt.

Då RJL har dokumenterat vissa delar av dataskyddsombudets ansvar anser vi att kravet är delvis uppfyllt. Dock finns ingen upprättad arbetsbeskrivning, en sådan bör upprättas så fort som möjligt, åtminstone i en reviderbar förstaversion.

GDPR tillämpar omvänd bevisbörda vilket kräver att RJL måste kunna visa på att de har ett dataskyddsombud med ett tilldelat ansvar samt att dataskyddsombudet inte tilldelats uppgifter av intressekonflikt. Risken med att inte ha upprättat en arbetsbeskrivning är att sanktioner tilldelas vid en eventuell tillsyn.

RJL bör säkerställa att arbetsbeskrivningen tydliggör mandat och inte riskerar att detaljstyra dataskyddsombudets arbete. En för snäv arbetsbeskrivning riskerar att effekten blir att dataskyddsombudet endast arbetar enligt specifika instruktioner vilket gör att relevanta uppgifter kan missas. Vidare bör RJL också säkerställa att dataskyddsombudet inte tilldelas arbetsuppgifter där det finns en risk för att dataskyddsombudet inte skulle kunna fullgöra sitt uppdrag och utföra sina uppgifter på ett oberoende sätt, där dataskyddsombudet till exempel behöver kravställa sig själv.

2.5. Har åtgärder vidtagits för att säkerställa att det hos medarbetarna inom förvaltningen/arna finns en tillräcklig kunskap om de krav som följer av dataskyddsförordningens ikraftträdande?

2.5.1. Iakttagelser

Ledningen och verksamhetsansvariga har fått en övergripande klassrumsutbildning (”Utbildningsmaterial_GDPR.pptx”) som har upplevts positiv under intervjuerna. Samtliga anställda har tillgång till en webbutbildning samt riktlinjer och mallar (se 2.1.1) på intranätet. Det ligger i varje chefs ansvar att dess anställda är tillräckligt informerade om GDPR. Ingen uppföljning har gjorts om de anställda har fått eller tagit till sig informationen.

Vi har inte fått ta del av någon information om kommande löpande utbildningar.

2.5.2. Bedömning

Vi bedömer att kontrollmålet delvis är uppfyllt.

Då samtliga anställda har möjlighet att ta del av information om GDPR på intranätet samt att de personer som behandlar känsliga uppgifter redan följer riktlinjer och rutiner under

patientdatalagen anser vi att RJL har vidtagit tillräckliga åtgärder för att säkerställa att medarbetarna har tillräcklig kunskap i dagsläget.

Vid nyanställning finns en checklista med punkter om informationssäkerhet den nyanställde måste läsa, där ska information ges om GDPR.

Dock saknar vi en utbildningsplan framåt med löpande utbildning och uppföljning av om de anställda faktiskt tagit del av och förstått innehållet. På grund av detta bedömer vi att RJL delvis har uppfyllt kravet.

2.6. Finns ett tillräckligt skydd för personuppgifterna, så att endast behöriga har tillgång till dem?

2.6.1. Iakttagelser

RJL har sedan länge arbetat med ett ledningssystem för informationssäkerhet(LIS) under för regionen gällande standarder, ex. ISO 27000 (En internationell standard för informationssäkerhet). Detta arbete inkluderar informationsklassningar och riskanalyser, såväl som rutiner för inbyggt dataskydd och dataskydd som standard inbegripet behörighetshantering.

Utöver ovan nämnt är organisationens informationssäkerhetsspecialister ute i organisationen och informerar om samt utbildar inom informationssäkerhet.

Under våra intervjuer har några verksamheter inom RJL har uttryckt att man upplever resursbrist inom informationssäkerhetskompetens på regionledningskontoret och att denna skulle behöva utökas för att samtidigt hinna med de åtgärder som krävs, både enligt tidigare standarder och GDPR.

En av de åtgärder GDPR kräver som RJL ännu inte hunnit med är konsekvensbedömning avseende dataskydd för högriskbehandlingar. Det finns enligt GDPR tre fall då man särskilt ska genomföra en konsekvensbedömning, dessa är följande:

1) En systematisk och omfattande bedömning av fysiska personers personliga aspekter som grundar sig på automatisk behandling, inbegripet profilering, och på vilken beslut grundar sig som har rättsliga följder för fysiska personer eller på liknande sätt i betydande grad påverkar fysiska personer.

2) Behandling i stor omfattning av särskilda kategorier av personuppgifter (personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning) eller av personuppgifter som rör fällande domar i brottmål och överträdelser.

3) Systematisk övervakning av en allmän plats i stor omfattning.

2.6.2. Bedömning

Vi bedömer att kontrollmålet delvis är uppfyllt.

RJL har sedan länge arbetat med informationssäkerhet och arbetar mot väletablerade standarder såsom ISO 27000. Det innebär att RJL har ett ledningssystem för informationssäkerhet som tagits fram baserat på standarder för informationssäkerhet på plats som ännu inte fullt anpassats efter GDPR.

Vi ser till exempel att ett resultat av att man inte hunnit med allt som krävts, är att har man skjutit på att genomföra konsekvensbedömningar avseende dataskydd (DPIA) för högriskbehandlingar. Dessa är centrala för att identifiera vilka dataskyddsåtgärder som måste vidtas för personuppgifter. Vi har inte sett någon plan om när metod, process och genomförande av konsekvensbedömningar ska upprättas och genomföras. På grund av att man inte genomfört dessa anser vi att RJL delvis uppfyllt kraven.

2.7. Har organisationen system och rutiner för att proaktivt upptäcka förlust eller läckage av personuppgifter?

2.7.1. Iakttagelser

Vad gäller IT-system för att proaktivt upptäcka förlust eller läckage av personuppgifter så utreder RJL möjligheten att aktivera funktioner för filtrering av e-post och internettrafik. Någon implementation har dock ännu inte gjorts.

Vidare har RJL ett implementerat LIS med incidenthanteringsrutiner där de anställda uppmanas att anmäla avvikelser. Rutinerna är likadana som tidigare men ett ytterligare val för att rapportera personuppgifter har adderats, vilket innebär att det är ett väl beprövat system inom organisationen.

2.7.2. Bedömning

Vi bedömer att kontrollmålet är delvis uppfyllt.

RJL arbetar aktivt med ett ledningssystem för informationssäkerhet mot organisationen inkl. utbildningar och informationsmöten på begäran av de anställda. I dessa fall ser vi att man arbetar proaktivt med utbildning samt uppmanar de anställda om att rapportera upptäckta förluster eller läckage.

Vi ser dock att ingen teknisk lösning är på plats och att risken med detta är att det till största sannolikhet resulterar i att eventuellt läckage eller förlust kommer att identifieras i efterhand. Vi rekommenderar därför starkt att utföra åtgärder för att proaktivt kunna identifiera förlust och/eller läckage.

Då dataskyddsförordningen inte explicit nämner att proaktiv teknisk monitorering behöver finnas på plats samt att RJL arbetar kontinuerligt med att informera verksamheterna om gällande informationssäkerhetsrutiner anser vi att RJL delvis uppfyllt kravet.

2.8. Finns system och/eller rutiner för att hantera den registrerades rättigheter?

2.8.1. Iakttagelser

Det finns ett styrdokument och en rutin på plats (”De_registrerades_rattigheter.docx”) om att kontakta regionjurist vid inkommen förfrågan avseende den registrerades rättigheter.

Vidare RJL har upprättat ett formulär som hanterar rätten till tillgång samt rätten till information på RJL:s hemsida[2].

Texten skulle kunna kompletteras med vilken rätt den registrerade har.

För rätten till rättelse, rätten till invändningar och rätten till begränsning kontaktas RJL enligt deras integritetspolicy på webben (länkad ovan), det finns dock inga internt upprättade riktlinjer eller rutiner för dessa rättigheter.

Vad gäller rätten till radering samt rätten till dataportabilitet har RJL ännu inte färdigställt en process då frågetecken kring offentlighetsprincipen kvarstår. Detta är något RJL för tillfället analyserar och arbetar på att lösa.

2.8.2. Bedömning

Vi bedömer att kontrollmålet delvis är uppfyllt.

RJL har tagit fram ett formulär som hanterar rätten till tillgång för den enskilde medborgaren. Vidare konstaterar vi att RJL har kompetensen på plats för att hantera övriga rättigheter ad hoc, dock behöver RJL ta fram, implementera och dokumentera process och metod för att hantera dessa. Dels för att kunna uppvisa vid en eventuell inspektion att man har det på plats och dels för att undvika sanktionsavgifter på grund av felaktigt handlande vid en rättighetsförfrågan.

Vi anser även att RJL bör köra tester på samtliga av rättigheterna för att säkerställa att RJL klarar av att hantera en begäran inom 30 dagar.

Med ovan anledning anser vi att RJL delvis har uppfyllt kravet.

2.9. Finns en ändamålsenlig organisation för incidenthantering utifrån dataskyddsförordningens krav?

2.9.1. Iakttagelser

RJL har sedan länge en gedigen process och stödsystem på plats för att rapportera incidenter. De har på grund av GDPR konfigurerat om systemet så att det nu är möjligt att rapportera personuppgiftsincidenter. Informationssäkerhetsspecialister är ute i organisat-

[2] https://www.rjl.se/om-oss/kontakta-oss/persondataskydd-och-dataskyddsombud/begaran-om-registerutdrag/

ionen om utbildar och informerar om informationssäkerhet och incidenthantering på begäran av de olika verksamheterna.

2.9.2. *Bedömning*

Vi bedömer att kontrollmålet är uppfyllt.

Då RJL arbetar aktivt med incidenthantering samt har uppdaterat deras verktyg och process för incidentrapportering anser vi att RJL har uppfyllt kraven.

2.10. Har konsekvensbedömningar gjorts på personuppgiftsbehandlingar som kan bedömas ha en påverkan på den registrerades rättigheter och friheter?

2.10.1. *Iakttagelser*

RJL har tittat på metoder samt upprättat en riktlinje avseende konsekvensbedömning. Dock har ingen konsekvensbedömning genomförts ännu då man medvetet valt att prioritera andra delar inom GDPR. Det finns sannolikt behandlingar inom RJL som bör bli föremål för konsekvensbedömning.

Av våra intervjuer inom ramen för granskningen framgår att konsekvensbedömning är ett relativt okänt område inom organisationen, med undantag för styrgrupp och dataskyddsombud.

2.10.2. *Bedömning*

Vi bedömer att kontrollmålet ej är uppfyllt.

Med beaktning till Datainspektionens senaste uttalanden i media[3] avseende konsekvensbedömning bör en metod fastställas samt konsekvensbedömningar genomföras så snart som möjligt, för att inte riskera att bli föremål för sanktionsavgifter.

Då RJL ännu inte fastställt någon metod eller genomfört någon konsekvensbedömning anser vi att kravet ännu inte är uppfyllt.

[3] https://digital.di.se/artikel/manga-riskerar-miljonboter-pa-grund-av-gdpr-miss

3. Revisionell bedömning

Granskningen syftar till att bedöma om:

- Regionstyrelsen har vidtagit tillräckliga åtgärder för att säkerställa att Region Jönköping följer lagstiftningen enligt GDPR

Vi bedömer att regionstyrelsen delvis har vidtagit tillräckliga åtgärder för att säkerställa att Region Jönköping följer lagstiftningen enligt GDPR. Det finns en medvetenhet hos regionledningen samt dataskyddsombudet om kvarvarande arbete där man medvetet har skjutit på vissa delar då andra delar varit högre prioriterade.

Vi rekommenderar att RJL fortsätter att arbeta aktivt med att implementera resterande åtgärder för att landa på en nivå som håller för kommande praxis.

PwC gör i dagsläget inget uttalande om RJL efterlever lagen eller inte då praxisfall inte har berörts.

Bilaga 1: Ordlista

Konsekvensbedömning avseende dataskydd/Data protection impact assessment (DPIA)
Om en typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige före behandlingen utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter.

Resultatet ska vara en risk- och behovsanalys av personuppgiftsbehandlingen som påvisar vilken nivå av dataskydd som krävs.

Dataportabilitet
Den registrerade ska ha rätt att få ut de personuppgifter som rör honom eller henne och som han eller hon har tillhandahållit den personuppgiftsansvarige i *ett strukturerat, allmänt använt och maskinläsbart format (ex. XML eller JSON)* och ha rätt att överföra dessa uppgifter till en annan personuppgiftsansvarig utan att den personuppgiftsansvarige som tillhandahållits personuppgifterna hindrar detta.

Ledningssystem för informationssäkerhet (LIS)
Ett Ledningssystem för Informationssäkerhet bildar grunden för att bedriva ett systematiskt informationssäkerhetsarbete i en organisation. Ett LIS kan bestå av policys, riktlinjer, rutiner, mål och processer som är relevanta för riskhantering och informationssäkerhet inom organisationen. Ett LIS uppbyggnad kan variera från organisation till organisation men är ofta baserad på de internationella standarderna i ISO/IEC 27000-serien.

2019-02-26

Jean Odgaard	Rasmus Poulsen
Uppdragsledare	*Projektledare*