Finansbranschens GDPR-utmaningar

- Förändringsarbetet i organisationen mer utmanande än IT- och säkerhetsfrågorna

En enkätundersökning om Finansbranschens syn på utmaningarna vid anpassning till nya dataskyddsförordningen som träder i kraft den 25 maj 2018

September 2017

Peter Åsén
Mindbanque AB

mind|banque
Biblioteksgatan 29 | SE-114 35 Stockholm | www.mindbanque.com

Sammanfattning

Resultatet av Mindbanques undersökning ***Finansbranschens GDPR-utmaningar*** ger en bild av att de största utmaningarna är inom *governance och organisation* följt av *rättigheter för registerförda* samt *IT-system och IT-säkerhet*.

Hantering av ej strukturerad data kräver förändringsledning och pekas ut som den största utmaningen följt av att fastställa processer och dokumentation. Dessa frågor lyfts troligtvis på grund av att en majoritet av de tillfrågade anser att GDPR inte fått det gehör inom organisationen som anses nödvändigt. Endast 27 % tror att deras organisation kommer att ha lanserat en tids- och kostnadseffektiv lösning inom området när de nya reglerna träder i kraft den 25 maj nästa år.

Att effektiva IT-system kommer att bli en avgörande faktor för en tids- och kostnadseffektiv hantering av GDPR är tydligt givet kraven för en homogen datahantering. Processer för det, exempelvis korrigering, radering och flytt av persondata ses som utmanande bland de flesta tillfrågade. Merparten av processerna kan standardiseras genom IT-system, dock behövs ett uppsatt ramverk för hanteringen. Organisationens förändringsbenägenhet är avgörande för lyckad efterlevnad av regelverket.

Om enkätundersökningen

Mindbanques undersökning är en introduktion på temat GDPR med fokus på implementationsutmaningar. Enkäten har under sommaren 2017 sänts till 22 personer som alla är ansvariga för, eller har en central roll i, implementeringen av den nya dataskyddsförordningen GDPR. Urvalsgruppen är GDPR-ansvariga från storbanker, fondbolag, nischbanker och nätmäklare. Av 22 respondenter har 12 besvarat frågorna.

Resultatet av undersökningen har som syfte att belysa de utmaningar som GDPR innebär med ett knappt år kvar till regelverkets ikraftträdande. Undersökningens resultat kan på så vis inspirera till förändring, från resursplanering till systemstöd och organisering, genom att läsaren kan urskilja vilka områden inom GDPR som branschkollegor uppfattar som mer utmanande än andra.

Inledning

Den nya dataskyddsförordningen**, General Data Protection Regulation (GDPR)** är en EU-förordning som träder i kraft den 25 maj 2018. Förordningen är ett resultat av flera års utredning där EU-kommissionen enats om en gemensam reglering för hanteringen av personuppgifter för EU:s medborgare. GDPR ersätter tidigare EU-direktiv vilket innebär att rådande svensk lagstiftning (PUL) ersätts.

Den nya förordningen har ett tydligt fokus på förbättrade villkor för registerförda. Reglerna innehåller exempelvis ökade krav gällande hantering och utlämnande av registerdata. Vidare kommer de nya regleringarna ställa ökade krav på IT-säkerhet och incidentrapportering till granskande myndighet, för svenska bolag Datainspektionen.

Företag och organisationer som inte uppfyller lagstiftningen kan åläggas vite om upp till 4 % av moderbolagets globala omsättning vid bristande hantering.

Enkätens syfte

Mindbanques GDPR-undersökning har som syfte att ge svar på:

- **Vad som bör prioriteras inom GDPR**
  Utifrån respondenternas svar kan läsaren identifiera vilka områden inom GDPR som branschkollegor uppfattar som mest utmanande, och därmed kräver större fokus och prioritet

- **Vilken kompetens som krävs för ett lyckat GDPR-arbete**
  Resultatet av undersökningen bidrar till idéer om var fokus, rent kompetensmässigt, bör riktas i organisationen i syfte att få till ett kvalitativt och långsiktigt hållbart införande av GDPR

Utvalda frågor för enkäten

Enkätens frågor hanterar GDPR-utmaningar inom tre områden. Totalt 10 frågor.

1. Governance och organisation
   - Processer och dokumentation
   - Ej strukturerad persondata
   - Dataminimering och operativt arbete
   - Leverantörer och samarbeten
   - Incidentrapportering

2. Rättigheter för registerförda
   - Samtycke
   - Transparens (redigera, radera och exportera persondata)

3. IT-system och IT-säkerhet
   - Processer för bevakning av intrång
   - Säkerställa IT-systems krav för intrång
   - Dataminimering, IT-system

Respondenten besvarar hur utmanande de anser att det är att hantera denna fråga på en fyrgradig skala från *Inte alls utmanande* till *mycket utmanande*. Om respondenten inte kan bedöma utmaningen finns även svarsalternativet *vet ej*.

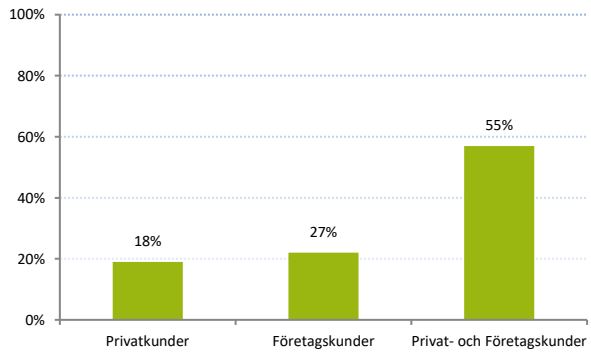
Målgrupp

Enkäten sändes till aktörer inom finansbranschen och till de ansvariga eller närmast berörda i arbetet med GDPR. I stora organisationer finns vanligtvis ansvariga för olika områden inom GDPR. I dessa fall har frågorna enbart ställts till övergripande ansvarig, exempelvis programledare.

Totalt sändes enkäten till 22 utvalda institutioner. Dessa är storbanker, nischbanker, försäkringsbolag, fondbolag och pensionsbolag. Totalt besvarades frågorna av 12 respondenter vilket motsvarar en svarsfrekvens om 54 procent.

Enkäten innehöll några frågor i syfte att förstå vilken kundgrupp verksamhet vänder sig till samt respondentens uppfattning om arbetet med GDPR har rimligt fokus idag.

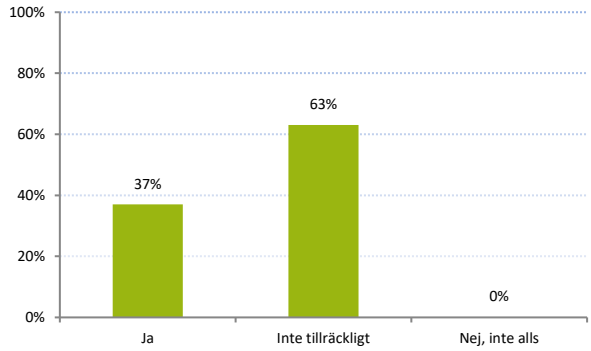
Till vilken målgrupp vänder sig er verksamhet?



Kommentar:

Merparten av respondenterna representerar företag som har både privat- och företagskunder.

Anser du att arbetet med GDPR i er verksamhet har rätt prioritering och fokus idag?

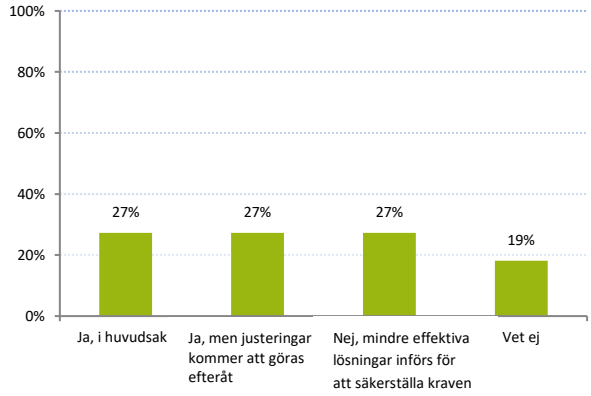


Kommentar:

Det är tydligt bland respondenterna att GDPR ännu inte nått den prioritet som anses nödvändig eller rimlig.

Det har även påpekats att frågan är svår att förankra inom organisationen då GDPR för många innebär ett nytt sätt att arbeta med persondata och personuppgifter. Det förändrade arbetssättet ställer nya krav på organisation, processer och IT-system. Dessa är redan idag fullt engagerade i andra prioriterade förändringsprojekt, exempelvis andra regelverksprojekt.

Tror du att ni kommer kunna hantera regelefterlevnad inom GDPR på ett rimligt och kostnadseffektivt sätt vid införandet 2018?



Kommentar:

Bland respondenterna bedömer var fjärde att de delvis tvingas införa mindre effektiva lösningar till den 25 maj 2018.

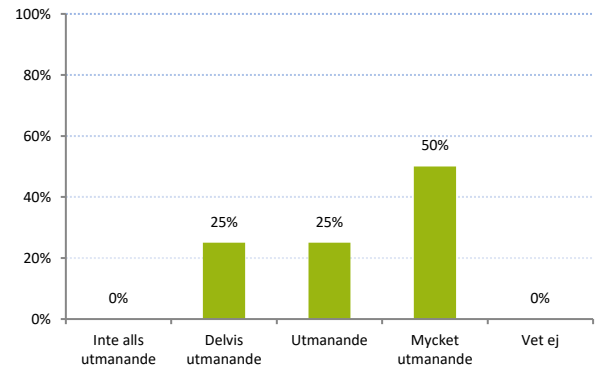
Detta antyder att en av utmaningarna i arbetet blir att prioritera vilka delar som är kritiska att efterleva, respektive mindre kritiska. Dessutom att kunna prioritera i dimensionen effektivitet där vissa anpassningar blir fulländade medan andra medvetet tillfälliga och mindre effektiva. Detta för att säkra projektets leverans inom given tidsram i maj 2018.

Redovisning av enkätresultatet

Resultatet av svaren redovisas i den ordning respondenterna ser den största utmaningen. Svaren redovisas sedan i fallande skala utifrån hur omfattande utmaningen uppfattats.

Hantering av persondata

Hur utmanande anser du att det är att säkerställa interna processer och dokumentation så att de uppfyller kraven gällande persondatahantering inom GDPR?

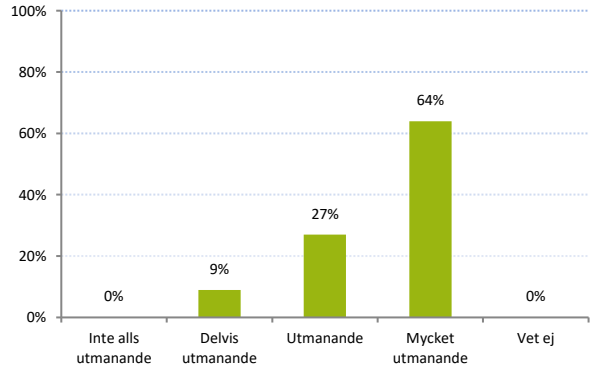


Kommentar:

GDPR ställer ökade krav på dokumentation av rutiner och processer som behandlar persondata.

Att formalisera ett ramverk att arbeta efter och där rutiner underlättar en säker och korrekt behandling av personuppgifter anses vara mycket utmanande. En anledning kan vara att implementeringen av GDPR ännu inte anses prioriterat i den utsträckning som projektledare anser nödvändig.

Hur utmanande anser du att det är att uppfylla kraven för att behandla persondata som ligger utanför strukturerade IT-system?



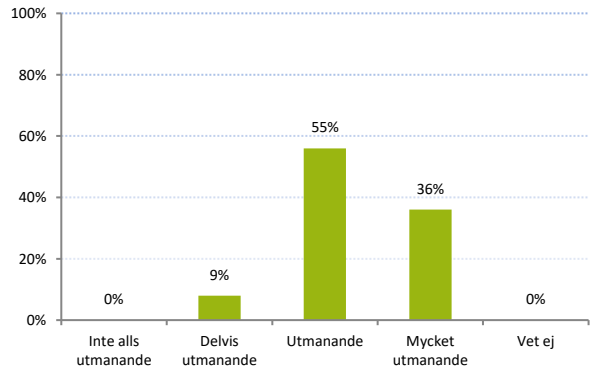
Kommentar:

Personuppgifter förekommer utanför strukturerade IT-system exempelvis i dokument eller i email. GDPR ställer krav på behandling av en registerförds samtliga personuppgifter, detta omfattar då även uppgifter som sparats utanför standardiserade IT-system.

Att hantera denna fråga ses som en stor utmaning bland de tillfrågade. Baserat på den s k missbruksregeln i PUL har många organisationer inte fokuserat på att inkludera ostrukturerat data i rutiner och policys, vilket gör att förändringsarbetet för att möta kraven i GDPR kan vara omfattande.

Export av data för registerförd

Hur utmanande anser du att det är att uppfylla kraven för att exportera data för registerförd?



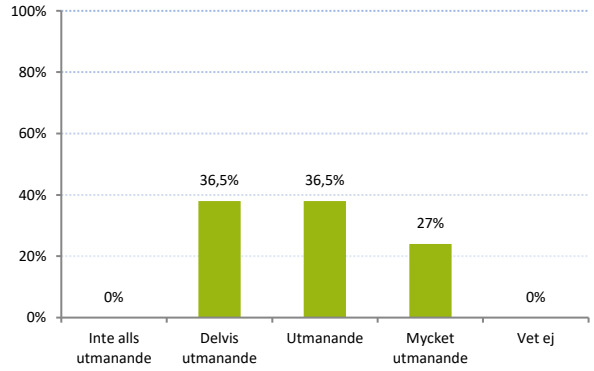
Kommentar:

En viktig fråga inom GDPR är att registerförda ska kunna ta med sig standardiserad data till en annan aktör, exempelvis vid byte av tjänst.

En tydlig majoritet anser att export av registerdata är utmanande eller mycket utmanande. Utmaningen tros ligga i att ta fram ett format som uppfyller kraven på läsbarhet och innehåll givet vilka krav som ställs.

Transparens för registerförd

Hur utmanande anser du att det är att uppfylla kraven för att hantera korrigering och radering av registerförd?



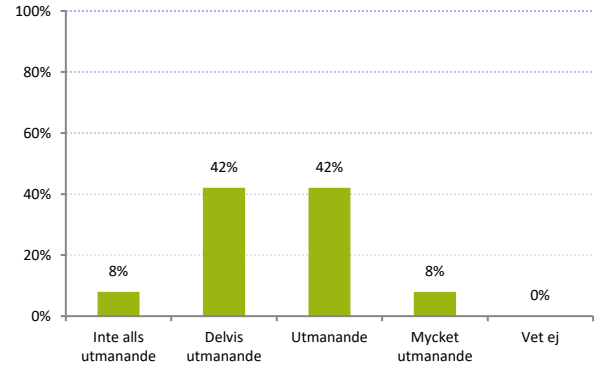
Kommentar:

Ökad transparens är en viktig del av det nya regelverket. Detta innebär att registerförda på ett enkelt sätt ska kunna ändra sina uppgifter, likväl radera uppgifter givet att inga andra regelverk hindrar detta.

Resultatet visar att det anses vara svårare att redigera och radera data än att hantera exempelvis samtycke för en registerförd. Detta kan bero på att samtycke förväntas lagras i ett standardiserat system inom organisationen, alltmedan berörda personuppgifter är spridda på ett antal olika IT-system vilka inte från början designats för att understödja en effektiv korrigerings- och raderingshantering. Att missbruksregeln i PUL försvinner så att även personuppgifter i s k ostrukturerat format träffas av regelverket bidrar sannolikt till att området anses utmanande.

Hantering av samtycke

Hur utmanande anser du att det är att uppfylla kraven gällande hantering av samtycke för registerförd?



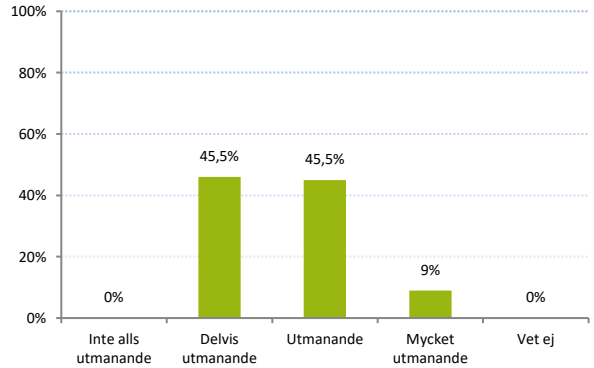
Kommentar:

Samtycke har en central roll inom GDPR. Registerförda ska dessutom ha möjlighet att på ett enkelt sätt återkalla samtycke för önskad aktivitet.

Samtycke anses vara mindre utmanande att hantera än korrigering och radering av registerdata. Detta kan bero på att flera aktörer redan idag har rutiner och effektivt IT-stöd för samtyckeshantering.

Hantering och lagring av enbart relevant persondata (dataminimering)

Hur utmanande anser du att det är att uppfylla kraven för att säkerställa att dataminimering efterföljs. Det vill säga att enbart persondata som är nödvändig för varje enskilt ändamål hanteras?



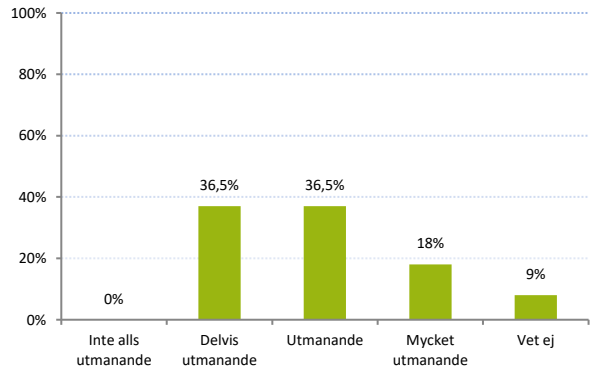
Kommentar:

Syftet med dataminimering är att säkerställa att endast för syftet behövlig information samlas in och att personer inom en organisation inte har tillgång till mer information om en registerförd än vad som anses nödvändigt för att hantera en arbetsuppgift. Detta innebär implementering av såväl utformning av IT-system som en behörighetshierarki för brukare.

Aktörer inom bank och finans förhåller sig redan idag till ett branschpraxis för personuppgiftshantering med stöd av banksekretessen. Detta innebär att aktörer redan idag i många fall arbetar strukturerat på temat dataminimering.

Leverantörer och samarbetspartners

Hur utmanande anser du att det är att uppfylla kraven för att säkerställa att leverantörer och samarbetspartners behandlar personuppgifter korrekt?



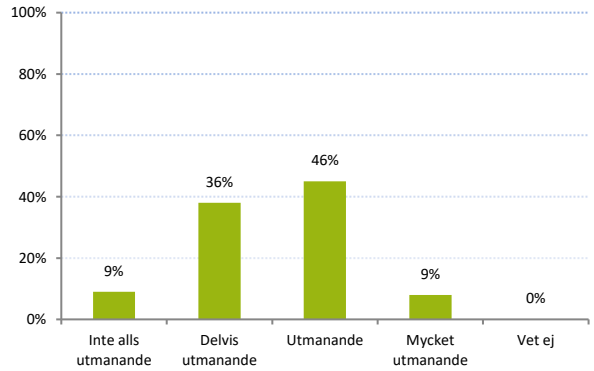
Kommentar:

Inom PUL äger samtliga aktörer som behandlar en uppdragsgivares kunddata ett ansvar för hanteringen av den. Inom GDPR flyttas detta ansvar till uppdragsgivaren som samlade in uppgifterna. Detta innebär att uppdragsgivare ansvarar för personuppgifternas hela kedja, vilket ställer ett ökat krav på leverantörers hantering av persondata.

Resultatet visar på att merparten av de tillfrågade har ett gott förtroende för sina leverantörer och för möjligheten att uppfylla kraven om säker hantering. Ansvarsfrågan hamnar förhållandevis långt ned på listan för utmaningar som regelverket för med sig.

IT-säkerhet

Hur utmanande anser du att det är att uppfylla kraven för att hantera processen för bevakning av intrång?

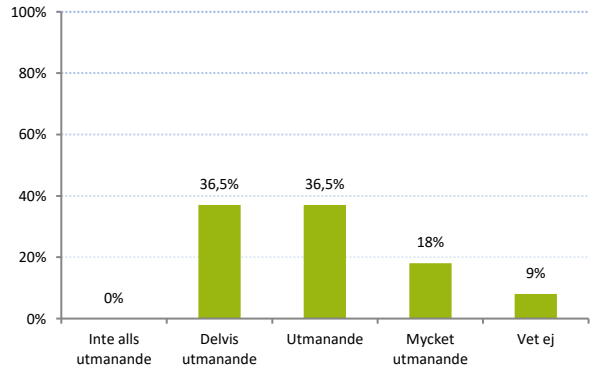


Kommentar:

Löpande hantering och bevakning av intrång ställer höga krav på en effektiv IT-organisation med möjlighet att identifiera angrepp och intrång.

Organisationer inom Bank och finans har redan idag ett behov av att hålla en hög IT säkerhet. Detta är tydligt då kommande rutinkrav anges vara mindre utmanade än flera andra förändringar.

Hur utmanande anser du att det är att uppfylla kraven för att säkerställa att IT-systemen klarar kraven inom IT-säkerhet



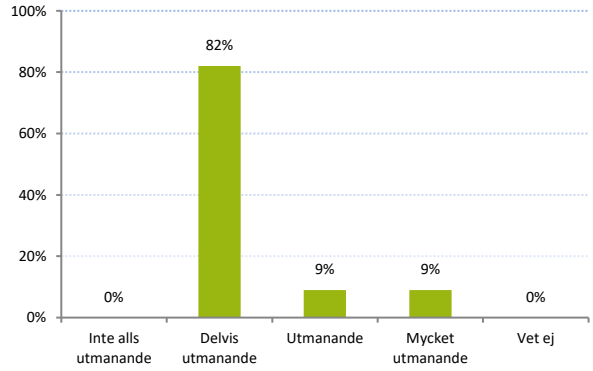
Kommentar:

GDPR ställer krav på att IT-system ska kunna hantera ett tillfredställande IT-skydd gällande säkerhetsfrågor.

IT-säkerhetsfrågan hamnar relativt långt ned på utmanandeskalan. En förklaring skulle kunna vara att flera operatörer förväntar sig att befintliga leverantörer säkerställer befintliga system för att uppfylla kraven inom GDPR. De respondenter som ser denna fråga som *mycket utmanande* kan exempelvis tänkas ha egna system som behöver anpassas internt.

Incidentrapportering

Hur utmanande anser du att det är att uppfylla kraven för att hantera rapportering av incidenter?



Kommentar:

Från och med den 25 maj ska incidenter och dess omfattning rapporteras till tillsynsmyndighet inom 72 timmar.

Det är tydligt att majoriteten av respondenterna inte ser incidenthantering enligt GDPR som utmanande. En trolig förklaring är att många bolag redan har en etablerad organisation och fungerande rutiner för hantering av incidenter, där rapportering till tillsynsmyndigheten inom en viss tidsgräns, kan implementeras förhållandevis lätt.

Avslutning

Undersökningen visar att samtliga respondenter bedömer att implementationen av GDPR är utmanande. Detta uttrycks inte enbart i enskilda svar utan även i undersökningen som helhet där 61 procent av svaren är inom kategorin *utmanande* eller *mycket utmanande*.

Governance och organisation anses vara det mest utmanande området. De ökade rättigheterna för registerförda rankas även högt i svårighetsgrad. Den praktiska lösningen i IT-system rankas däremot lägre.

Resultatet av undersökningen är delvis i linje med Mindbanques förväntningar. Organisationers bitvis låga prioritering av GDPR visar på att djupet av kunskapen om det nya regelverket skiftar i branschen. Om prioriteringen inom organisationen är låg leder det ofta till att förändringen av interna processer och rutiner inte blir effektiv. GDPR handlar inte enbart om en teknisk lösning, utan påverkar hela organisationer. En låg prioritering av GDPR nu, leder till att de lösningar som kommer att finnas på plats per 25 maj 2018 löper risk att bli mindre effektiva och i förlängningen mer kostsamma än annars.

Att hantering av ej strukturerad data anses vara en utmaning är förståeligt eftersom många utifrån den så kallade missbruksregeln i PUL inte ägnat området någon större uppmärksamhet tidigare till skillnad från områden som träffats av PUL sedan länge. Vidare är det även förståeligt att finansbranschen ofta har god IT-säkerhet och rutiner för identifiering av intrång varför dessa frågor känns något mindre utmanande.

Vad som emellertid är mer notabelt är att kravet att säkerställa att leverantörer och samarbetspartners som på uppdrag behandlar personuppgifter inte ses som lika utmanande som andra områden. Skälen kan övergripande sett vara tre:

- Många har redan väl passande ansvarsstruktur för GDPR som stöds av avtal och överenskommelser
- Antalet leverantörer och samarbetspartners är begränsat och arbetet med att anpassa ansvarsfördelning och tillhörande avtal tros kunna vara begränsat
- När respondenterna svarade på frågorna hade ämnet ej ännu belysts i lika hög grad som andra områden

Enkäten besvarades i slutet av juni och i första hälften av augusti 2017. Sedan dess har tecken i branschen noterats avseende upplevda utmaningar bl a i arbetet med att identifiera och avtala avseende personuppgiftsansvar, vilket kan indikera att området idag skulle kunna ha bedömts utgöra en större utmaning än var fallet för en tid sedan.

Som beskrivits ovan bedömde respondenterna sammantaget att GDPR-implementeringen är utmanande, och då speciellt området governance och organisation. Organisationer där verksamheten varit väl inarbetad vad avser PUL synes ha lättare att ta till sig och implementera GDPR än andra.

Projekten handlar mycket om dokumentation och IT liksom om förändring av organisationers syn på behandling av personuppgifter vilket inkluderar policys, instruktioner och annan dokumentation. Kontrollfunktioner i organisationen fungerar avsevärt mycket bättre när de operativt och kulturellt har etablerat den förändring som förordningen för med sig. Förändringsledning är därmed en viktig och värdefull kompetens i GDPR-projekten.

Vid frågor om undersökningen är du välkommen att kontakta Peter Åsén, peter.asen@mindbanque.com.

Om Mindbanque

Mindbanque är en strategi- och förändringskonsult med fokus på den nordiska finanssektorn. Mindbanque erbjuder konsulter inom förändringsledning och som verksamhetsexperter med gedigen erfarenhet att tolka och implementera nya regelverk.

Kunderna representerar många av finansindustrins olika roller, exempelvis banker och försäkringsbolag, kapitalförvaltare och fondbolag eller investmentbanker och fondkommissionärer.

Kundens behov sträcker sig från tidiga skeden i ett förändringsarbete till ett färdigt genomförande. Konsulter på Mindbanque har ofta roller som projektledare, kravanalytiker och verksamhetsexpert.