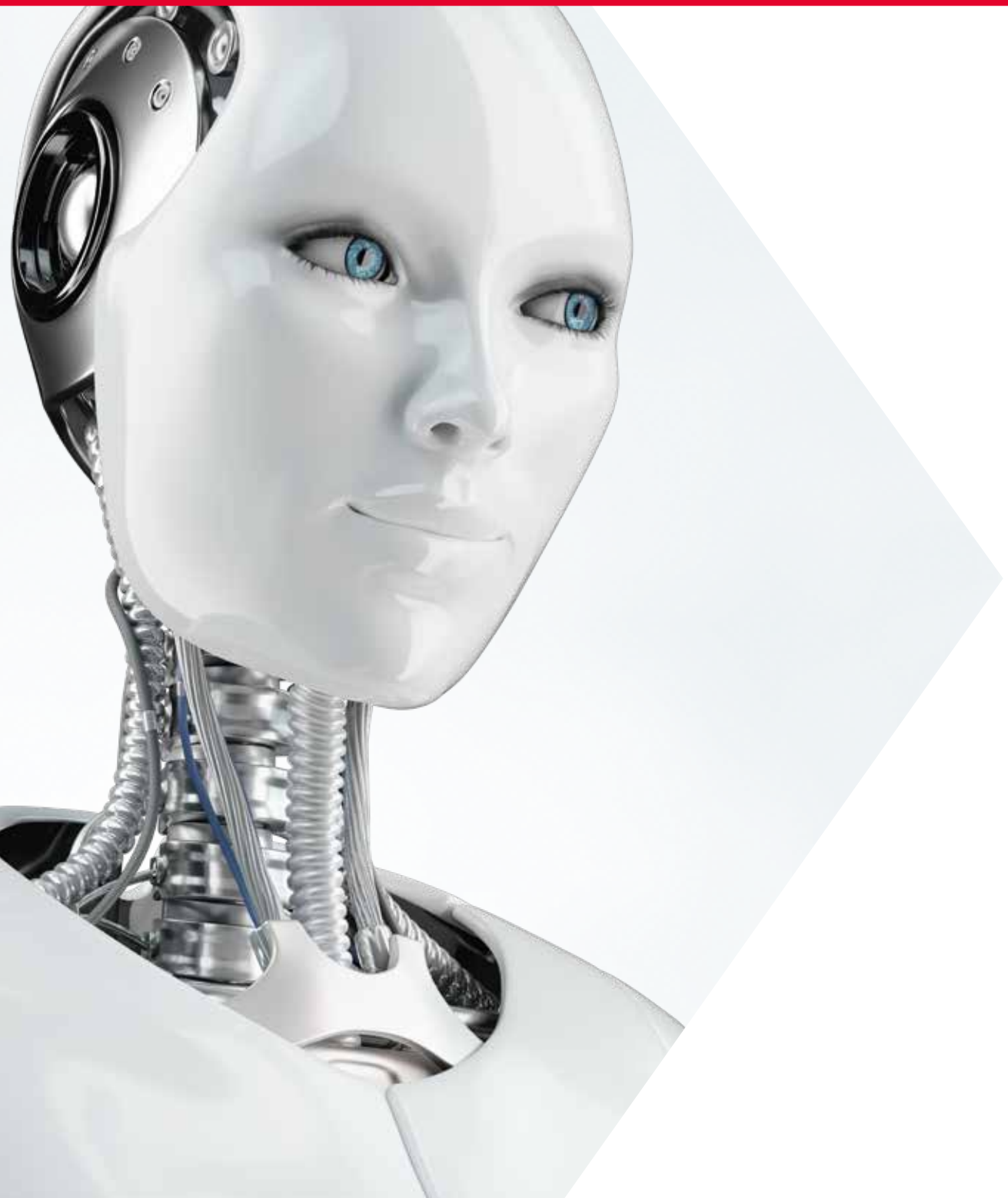


Intelligent dokumentförstöring

För en GDPR kompatibel generation

Varför dokumentsäkerhetspolicy är en integrerad del av GDPR

Friskrivning
Inget innehåll i detta dokument ska betraktas som juridisk rådgivning. Organisationer bör anlita juridiska rådgivare rörande efterlevnad av den allmänna dataskyddsförordningen eller andra tillämpliga lager eller förordningar.

BLI GDPR REDO*

*Dokumentförstöring är en del av GDPR kravet

› **Om** detta dokument

Syftet med detta dokument är att ge en översikt över vad GDPR står för och vilka utmaningar företag står inför samt erbjuder ett ramverk för att effektivt följa den nya dataskyddsförordningen.

Syftet med detta dokument är att ge en introduktion till EU:s allmänna dataskyddsförordning (GDPR) och hur den påverkar olika verksamheter, så att du kan utveckla ett ramverk för den egna verksamhetens säkerhetspolicy avseende papper nu när de nya förordningarna har trätt i kraft.

Vad är GDPR? Den kräver att organisationer tillämpar sund säkerhetspraxis kring elektronik- och pappersbaserade data, och i händelse av dataintrång meddela berörda eller potentiellt berörda personer.

GDPR har en global räckvidd till alla organisationer som kontrollerar eller bearbetar identifierbara personuppgifter om personer inom EU, oberoende av var dessa organisationer finns rent geografiskt. GDPR-kraven gäller både elektronik- och pappersbaserade personuppgifter och betyder att alla organisationer ska tillgodose GDPR-kraven om de hanterar identifierbara personuppgifter med ursprung inom EU.

Även om elektronisk datasäkerhet har hög prioritet hos många organisationer så är det vanligt att man inte på ett adekvat sätt hanterar säkerheten kring pappersbaserade data. Faktum är att nästan två tredjedelar av kontoren medger att man inte strimlar konfidentiell information1. Detta gör att organisationer riskerar att inte efterleva GDPR och att data läcker ut och riskerar ledas till bedrägerier och identitetsstöld. Rexel, ett ledande varumärke inom dokumentförstörare,uppmuntrar organisationer att granska sin säkerhetspolicy och praxis till både pappersbaserad och elektronisk data.

DEN ALLMÄNNA DATASKYDDSFÖRORDNINGEN (GDPR)

En översikt

GDPR syftar till att skydda den enskildas integritetsrättigheter i Europa, oavsett om det gäller EU-medborgare eller inte. Dessa integritetsrättigheter innefattar, men begränsas inte till:

Transparens
Rätten att få tydlig information om hur organisationer bearbetar personinformation.

Ökad kontroll
Rätten att kontrollera hur organisationer använder personlig information

Ökad säkerhet
Rätten till information om hur organisationer på ett adekvat sätt skyddar personinformation.

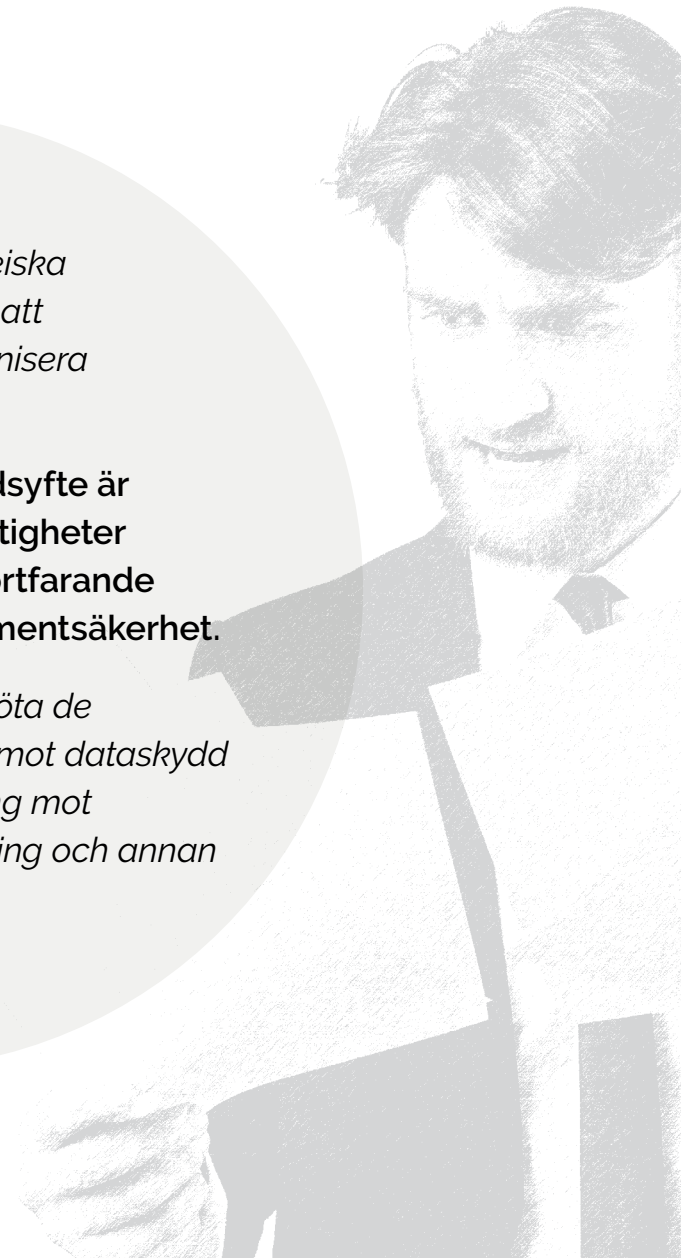
Begränsning av insamling och användning av data
Rätten att förvänta sig att organisationer minimerar insamling och användning av information.

Meddelande vid dataintrång
Rätten till information vid ett dataintrång.

GDPR ingår i den Europeiska kommissionens plan för att modernisera och harmonisera dataskyddsreglerna.

Även om GDPR:s huvudsyfte är att stärka integritetsrättigheter digitalt så gäller den fortfarande pappersbaserad dokumentsäkerhet.

Fokus ligger på att bemöta de växande utmaningarna mot dataskydd och sekretess, exponering mot säkerhetsintrång, hackning och annan olaglig hantering.



DEN ALLMÄNNA DATASKYDDSFÖRORDNINGEN (GDPR)

Vad har förändrats?

Följande punkter identifierar de specifika områden inom GDPR som innebär nya rättigheter för enskilda personer eller att nuvarande rättigheter under dataskyddslagen (Data Protection Act, DPA) har stärkts som en del av GDPR:

Dataöverföring och rätten att bli borttagen

- Enskilda personer har nu rätt att transportera sina personuppgifter från en organisation till nästa.
- Personuppgifter måste tillhandahållas i ett strukturerat maskinläsbart format.
- En person kan begära att personuppgifter raderas eller tas bort.

Information vid dataintrång

- Alla intrång ska rapporteras till ansvarig myndighet.
- Även enskilda personer som påverkas av intrånget ska informeras.

Register

- Lokala myndigheter behöver inte längre informeras om att personuppgifter bearbetas.
- Organisationer måste upprätthålla ett register över bearbetningsaktiviteter under deras ansvar.

Data Protection Impact Assessments and security

- DPIA:er är ett sätt att identifiera höga risker rörande enskildas integritetsrättigheter.
- Säkerhetskrav och -rekommendationer ska baseras på en riskbedömning.

Dataförvaltning och ansvar

- Organisationer måste även kunna visa att GDPR efterlevs.

Icke-efterlevnad av GDPR kan resultera i böter på upp till 20 miljoner Euro, eller 4 % av företagets globala intäkter, beroende på vilket belopp som är störst. Vidare har en registrerad person rätt att stämma en organisation inför domstol.

DEN ALLMÄNNA DATASKYDDSFÖRORDNINGEN (GDPR)

Vem gäller det?

Införandet av GDPR i maj 2018 påverkar personer med följande befattningar:

Registeransvariga
De anger hur och varför personuppgifter bearbetas

Dataskyddsansvarig
De agerar på registeransvarigas vägnar

Dessa två personer ansvarar för att säkerställa att deras klienter fullständigt efterlever alla aspekter inom GDPR för att undvika utkrävande av böter. En registerförare eller registeransvarig kan utse en dataskyddsansvarig och hålla register över alla bearbetningsaktiviteter som genomförs på klienters vägnar.

GDPR omfattar personuppgifter och känsliga personuppgifter i elektroniska och fysiska format

GDPR omfattar personuppgifter och känsliga personuppgifter i elektroniska och fysiska format

Det är viktigt att tänka på vilka typer av data GDPR kommer att gälla,vid framtagandet av en efterlevnadspolicy för organisationen.

Data som omfattas av GDPR innefattar information om en identifierbar person. Bland exemplen på personuppgifter som faller under GDPR finns fullständigt namn, e-postadress och telefonnummer.

GDPR tillämpar även extra skydd av en underkategori personuppgifter, som kallas känsliga personuppgifter.

GDPR avser personuppgifter som hanteras av organisationer i både elektroniska och fysiska format, som t.ex. pappersdokument.

Ett företagsregelverk för att följa GDPR

Organisationer har tre huvudområden som måste granskas för att uppnå GDPR. Genom att ta itu med dessa tre delar kan verksamheterna skapa tydliga ramverk för en datasäkerhetspolicy, vilket underlättar efterlevnad på alla områden av GDPR.

De tre delarna är:

Personalen

Personalens delaktighet och ansvar för all data som de bearbetar inom organisationen är avgörande. En organisation måste sätta tydliga regler och ramar för varje enskild anställd för korrekt hantering av all elektronik- eller pappersbaserad data. Dessa regler gör att GDPR kraven rörande hantering av alla data uppfylls i praktiken. Exempelvis kan du vilja införa tydliga regler kring användning av pappersdokument med känslig information och processen för korrekt makulering av det använda dokumentet, baserat på känslighetsnivån.

Processer

Detta rör processerna inom organisationen. Exempelvis att hantera användningen av data, såsom bearbetning eller lagring av kunddata. Det är avgörande att verksamheterna granskar alla sina aktuella datarelaterade processer. När brister och svagheter inom de befintliga processer har identifierats måste en ramverksplan utformas av den verksamhet som vill stärka, eller vid behov ersätta, dessa områden så att GDPR efterlevs.

IT och Teknik

Även nuvarande IT-kapaciteter och krav ska granskas och justeras på lämpligt sätt. Det är de enskilda verksamheterna som ska säkerställa att befintliga system som inte till fullo stödjer förordningarna antingen förbättras eller ersätts för att undvika dryga böter.

Varför är dokumentsäkerhet viktig?

Vi har diskuterat vad GDPR kräver att verksamheter gör, och nu är det relevant att ta upp frågan om dokumentsäkerhet inom organisationer och varför det är en viktig fråga för att möta GDPR:s krav.

Faktum är att en PwC-rapport från 2014, tillsammans med registerhanteringsföretaget Iron Mountain2 – som undersökte hur europeiska företag i mellansegmentet uppfattade och hanterade sin informationsrisk – visade att två tredjedelar av de svarande sade att riskhantering rörande pappersregister var topprioriterat.

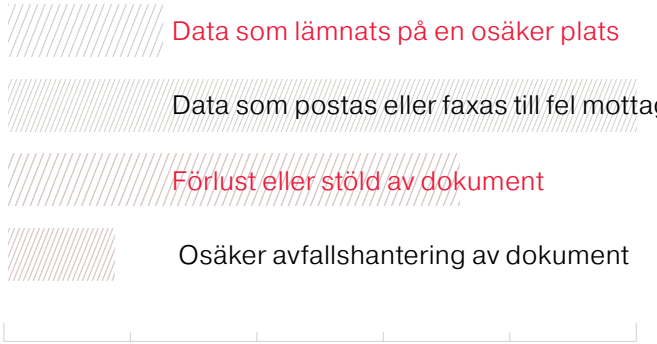
Även om digitala hot står högt på en organisations dagordning, så vore det ett misstag att anta att pappersbaserade säkerhetsrisker inte längre finns

Dokument utsätts fortfarande för många vanliga säkerhetsintrång

Av 598 datasäkerhetsincidenter som noterades mellan juli och september 2016 av den brittiska tillsynsmyndigheten för dataskydd, Information Commissioner's Office (ICO) kunde man se att:

14% berodde på förlust eller stöld av utskrivna dokument, ytterligare **19%** postades eller faxades till fel mottagare och 4% berodde på att data förvarades på en osäker plats. Ytterligare 3 % berodde på osäker makulering av papper. Så trots en exponentiell ökning av digitala tekniker kunde **40 %** av incidenterna hänföras till papper[3].

40% **av brittiska datasäkerhetsincidenter kunde hänföras till papper**



Registrerade incidenter rörande papperssäkerhet

Medvetenhet bland personalen är avgörande för att GDPR efterlevs

Om vi kommer fram till att papperssäkerhet är fortsatt avgörande för informationssäkerhet, så är frågan:

Vad kan organisationer göra åt detta?

Rexel är specialiserat på att tillhandahålla dokumentförstörare till organisationer, med möjlighet att samarbeta direkt med organisationer som t.ex. Kensington, världsledande inom fysisk säkerhet för IT-hårdvara vid delning av konsumentinsikter, vilket gett oss värdefulla insikter i de behov, önskemål och utmaningar som organisationer ställs inför när de vill skydda sig själva och efterleva kraven i GDPR.

Med denna kunskap ser vi två huvudsakliga orsaker till att man inte får till en effektiv hantering av dokumenthantering ute på företagen:

Brist på kunskap

Verksamheter bortser från betydelsen av papper på en alltmer digital arbetsplats och tar sig därför inte tid att bemöta de säkerhetsfrågor som kopplas till pappersdokument. Även om det finns en införd policy kan medvetenheten vara bristfällig om förordningen inte kommuniceras effektivt på alla verksamhetsnivåer.

Det måste vara enkelt

Tillgängligheten på lämpliga dokumentförstörare är avgörande för att en effektiv policy för dokumentförstöring ska lyckas. Alltför ofta förlitar sig organisationer eller kontor på ineffektiva manuella dokumentförstörare som inte uppfyller kraven, vilket gör att anställda inte kan makulera dokument effektivt och produktivt.

När man har kartlagt de bakomliggande orsakerna till utebliven dokumenthantering är nästa steg att skapa en process.

Lösning ett för att möta GDPR kraven

Brist på kunskap

Anställda utför i regel åtgärder som deras chefer tydligt markerar som prioriterade.

Med tanke på detta kan ineffektivitet åtgärdas med en tydlig och bestämd policy för makulering av dokument.

Med tanke på detta kan ineffektivitet åtgärdas med en tydlig och bestämd policy för makulering av dokument. I undersökningen som PwC/Iron Mountain gjorde 2014 av europeiska företag i mellansegmentet2 framgår att endast

40% har tydliga riktlinjer för de anställda rörande intern förvaring och arkivering av fysiska dokument, och endast 27% har företagspolicyer för säkerhet, förvaring och arkivering av konfidentiell information.

Lösning två
för att möta GDPR kraven

Det måste vara enkelt

Ett annat vanligt skäl till att medarbetare inte efterlever kraven på dokumentförstöring är att makuleringen är svår och tidskrävande.

Även om anställda har tillgång till dokumentförstörare är det inte alla som strimlar erforderliga dokument om det tar för lång tid eller är svårt att hantera.

Föga förvånande vill ingen organisation investera i dokumentförstörare som deras anställda troligen inte använder på grund av dålig produktivitet eller barriärer mot enkel användning, så dessa frågor bör lösas för att säkerställa maximal användning.

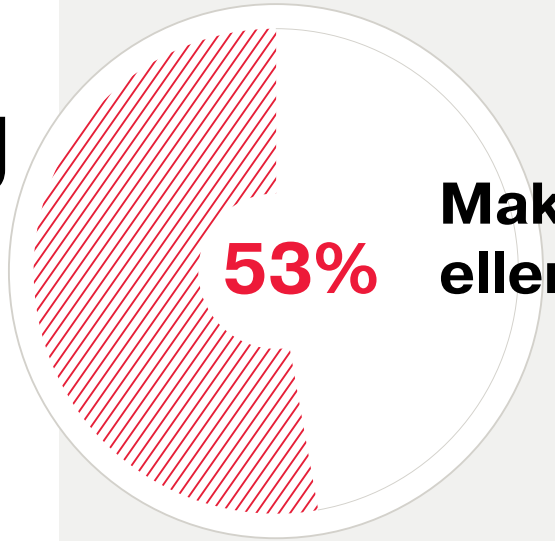
Öka de anställdas produktivitet med automatisk inmatningsteknik

Sammanfattning

Få din dokumentsäkerhetspolicy att fungera med Auto+ SmarTech dokumentförstörare.

Våra Auto+ SmarTech automastiska dokumentförstörare möjliggör övervakning och underhåll på flera platser och är ett direkt svar för att uppmuntra personalen att följa policyn för dokumentsäkerhet. Undersökning4 visar att 53% av medarbetarna samlar ihop en bunt med dokument innan man anser att vägen till dokumentförstöraren känns befogad.

Genom att tillåta personalen att makulera hela pappersbuntar fann en oberoende forskning att personalen kunde spendera 98% mindre tid vid maskinen5 och vara mer benägna att makulera mer frekvent.



Makulera i omgångar eller allt på en gång

14 min. 25 sec.
Manuellt

14 sec. med
Rexel Auto+
dokumentförstörare

Tid det tar att makulera 500 ark

6 viktiga GDPR -punkter att ha i åtanke

1. Överväg att utse en dataskyddsansvarig

Denne befattningshavare måste fullständigt uppfylla organisationens ansvar rörande GDPR och ha god förståelse för vilka data inom organisationen som räknas som ”personliga”, var de förvaras, vem som har tillgång till dem, hur man upptäcker intrång när de sker och till vem sådana ska rapporteras.
Den dataskyddsansvarige behöver inte vara en anställd – du kan outsourca denna funktion.

2. Bedöm dina system

Granska alla kontrakt, teknisk support, procedurer och verktyg som har att göra med bearbetning, hantering, lagring och radering av data så att du kan identifiera eventuella svagheter eller brister som kräver att förändringar görs.

3. Utveckla en strategi

Konstruera en ny strategi som säkerställer att GDPR efterlevs till fullo. Denna strategi kan innefatta nya investeringar i teknik, revidering av personalprocedurer och ansvar för databearbetning samt skapande av nya roller inom organisationer.

4. Implementera en ny organisationspolicy

Nästa steg mot GDPR-efterlevnad är att sätta planen i verket på alla nivåer inom organisationen. Investera i och introducera ny teknik och nya system som behövs på arbetsplatsen samt publicera en informativ guide till datahantering och bearbetning.

5. Anställdas engagemang

Presentera din nya efterlevnadspolicy C169för hela personalen; erbjud utbildning, information och vägledning så att de anställda är kunniga och medvetna om de förändringar som sker och deras ansvar för att säkerställa att företaget uppfyller kraven i GDPR.

6. Granska och förbättra

Efter att ha lanserat GDPR-planen, bör den kontinuerligt ses över och förbättras, även efter att förordningarna trätt i kraft. Genom att kontinuerligt identifiera eventuella nödvändiga förbättringar kommer du med framgång att kunna säkerställa att din organisation är helt överens med den nya lagen.

Källor

1 envirowaste.co.uk/blog/articles/third-companies-shred-private-documents

2 Beyond good intentions: The need to move from intention to action to manage information risk in the mid-market, PwC report in conjunction with Iron Mountain, June 2014

3 ico.org.uk/action-weve-taken/data-security-incident-trends

4 Evaluating Auto Feed Shredders. Prepared for ACCO Brands by Deep Blue Insight

5 Independent test from Intertek Testing & Certification Ltd June 2012

- Max saving when using an Auto+ 500X with SmarTech compared to a traditional feed shredder in a similar price level
- Research shows it takes an average of 14 minutes and 25 seconds to manually insert 500 sheets of paper into a traditional, manual-feed-shredder – but only 14 seconds to load the same number of sheets into an Auto+ 500X with SmarTech

www.rexeleurope.com

För mer information, vänligen kontakta

Acco Brands
Sundbybergsvägen 1

171 73 Solna