Viktiga riktlinjer för GDPR-efterlevnad

Brought to you by hp

Innehåll

Inledning

Det är dags att implementera inbyggd integritet

Den 25 maj 2018 träder EU:s allmänna dataskyddsförordning i kraft. Den kommer att ersätta all nationell dataskyddsreglering inom EU och alla som bedriver affärsverksamhet på den inre marknaden måste följa dessa regler. Den omfattar även företag utanför EU som gör affärer med kunder inom EU.

Under GDPR måste alla överträdelser mot personuppgiftsskyddet rapporteras inom 72 timmar från det att överträdelsen kommit till känna. Underlåtenhet att göra detta eller motbevisa försummelse, kan leda till böter på upp till 20 miljoner euro eller 4 % av den globala omsättningen, beroende på vilket som är högre.

Lyckligtvis kommer de åtgärder som krävs för att skydda företagets data som helhet även att hålla kundernas data säkra. Samma metod för klientsäkerhet med flera lager som vi på HP redan rekommenderar, bidrar till att säkerställa överensstämmelse med GDPR.

I denna e-guide tittar vi närmare på de viktigaste komponenterna i GDPR som IT-anställda behöver känna till, samt på hur ett enhetsstyrt klientsäkerhetsprogram kan bidra till regelefterlevnad.

En beskrivning av GDPR

De viktigaste punkterna för IT

Det finns i huvudsak två viktiga aspekter i GDPR: att skydda registrerade EU-medborgares rättigheter och att skydda registrerade EU-medborgares integritet. Båda medför tekniska konsekvenser.

För officiell information, läs den fullständiga texten. Men som IT-beslutsfattare behöver du känna till följande punkter:

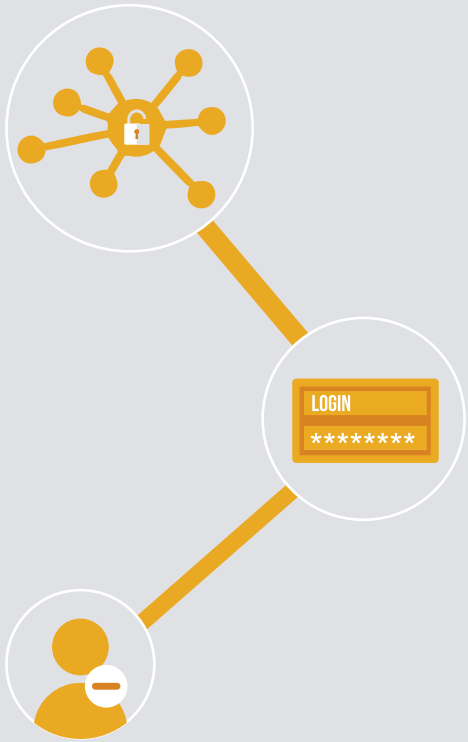
1. **Överträdelse måste rapporteras inom 72 timmar**
   Skulle ett dataintrång inträffa måste det rapporteras inom 72 timmar efter att det kommit till känna. Straffen för underlåtenhet att göra detta är hårda (se ”Vilka är påföljderna för bristande efterlevnad?”)

2. **Rätten att bli bortglömd**
   Alla EU-registrerade individer har rätt att bli bortglömda i systemen. Vid en förfrågan måste du radera deras data inklusive alla kopior

3. **Rätten till dataportabilitet**
   EU-medborgare har rätt att kontrollera sina egna uppgifter. På begäran måste du överlämna deras uppgifter i ett format som är tillgängligt för dem, så att de kan överföra dem till en tredje part

4. **Internationell överföring**
   Att flytta personuppgifter till en annan datajurisdiktion (dvs. utanför EU) kan endast göras med uttryckligt medgivande och endast till en myndighet som anses ”adekvat”, eller med ytterligare säkerhetsåtgärder[1]

5. **Inbyggd integritet**
   Organisationer måste anta en egen strategi för inbyggd integritet som integrerar datasäkerhet i produkter, processer och tjänster som standardrutin[2,3]



Vem gäller GDPR för?

GDPR gäller alla företag som samlar in uppgifter och/eller bearbetar personuppgifter för EU-medborgare. Detta inbegriper organisationer som är baserade utanför EU som har verksamhet inom EU.

[1]https://iapp.org/news/a/top-10-operational impacts-of-the-gdpr-part-4-cross-border-data-transfers/ [2]Allen & Overy – The EU General Data Protection Regulation 2016
[3]http://www.computerweekly.com/news/450296306/10-key-facts-businesses-need-to-note-about-the-GDPR

En beskrivning av GDPR

Vad betraktas som ”personuppgifter”?

Enligt GDPR avser personuppgifter ”alla uppgifter som kan användas för att identifiera en person”.

Detta inbegriper genetisk, mental, kulturell, ekonomisk eller social information, tillsammans med det som traditionellt anses vara identifierande personuppgifter.

Detta kan medföra att organisationer som tidigare inte omfattades av dataskyddslagstiftningen nu faller inom ramen för GDPR.

Vilka är påföljderna för bristande efterlevnad?

Det högsta bötesbeloppet är 20 miljoner euro eller 4 % av den globala omsättningen, beroende på vilket som är högre. Detta gäller för de allvarligaste överträdelserna enligt förordningen, t.ex. underlåtenhet att anmäla ett säkerhetsbrott inom 72 timmar efter att det kommit till känna.

För mindre allvarliga överträdelser är bötesbeloppet högst 10 miljoner euro eller 2 % av den globala omsättningen. Kostnaderna för bristande efterlevnad är således betydande.

Checklista för GDPR-procedurer

Inom ramen för er datastyrning behöver ni tydliga rutiner för:

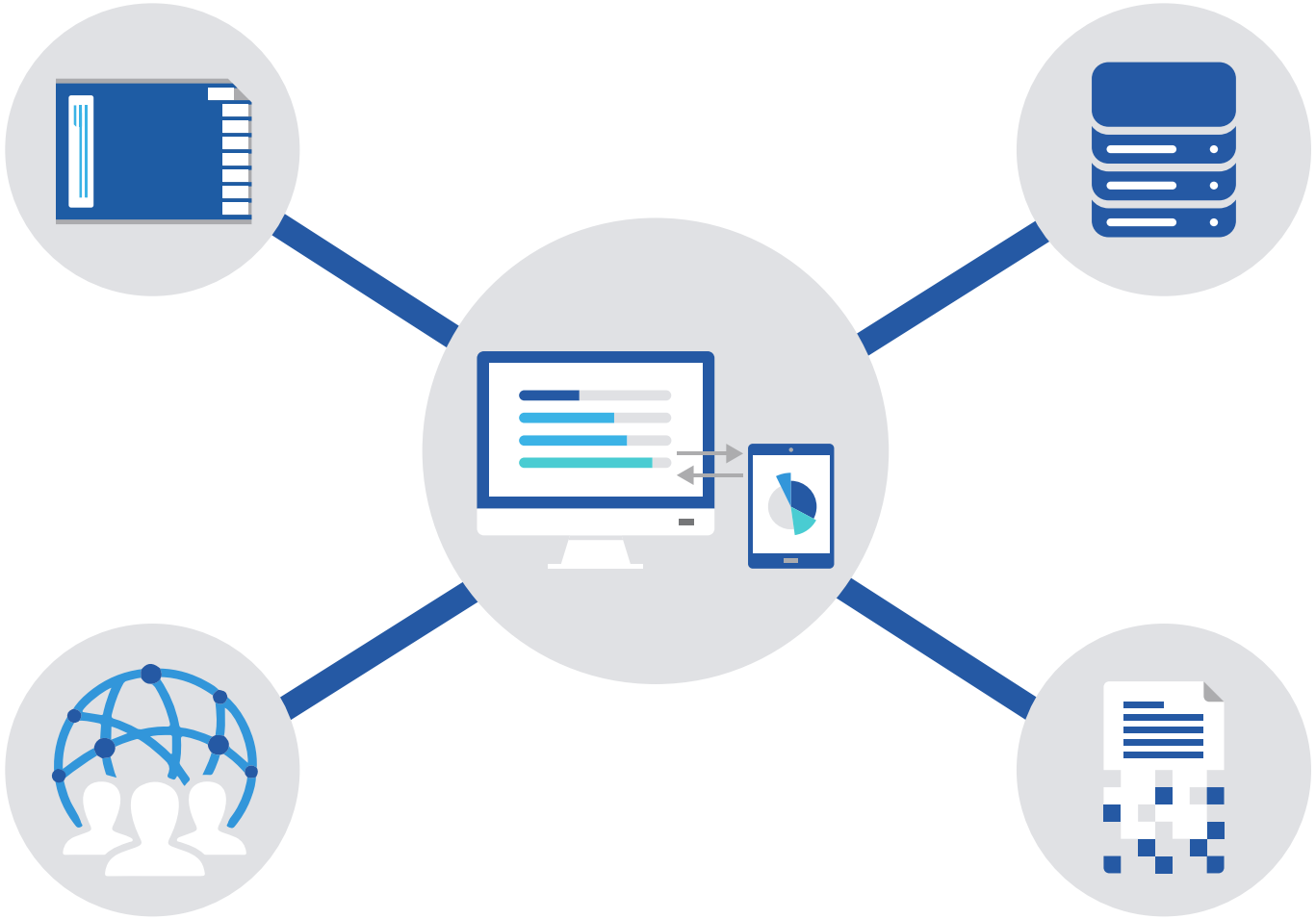
- Att informera de registrerade om hur deras uppgifter kommer att samlas in, lagras och bearbetas
- Erhålla de registrerades uttryckliga samtycke till detta
- Förse registrerade medborgare med deras data i ett format som är tillgängligt för dem
- Radera alla registrerade medborgares personliga data, inklusive kopior
- Överföra data till en annan granskare eller bearbetare
- Överföra data utanför EU, inklusive inom organisationen

Tekniska utmaningar för efterlevnad

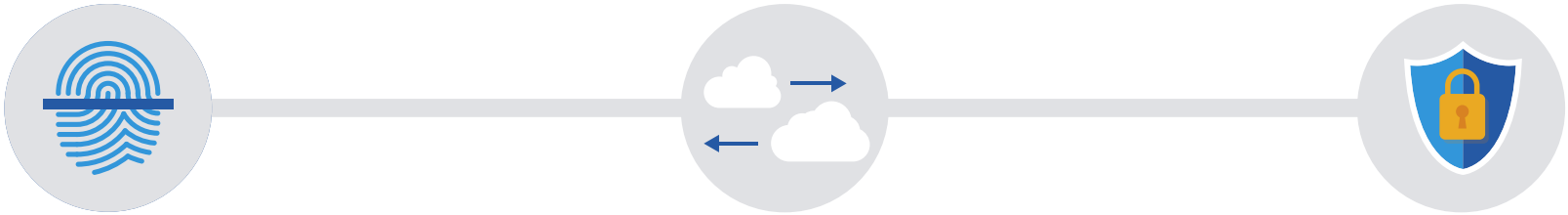
De största utmaningarna med GDPR är tekniska.

Att möjliggöra säker dataportabilitet, skydda individers data och deras rätt att bli glömda kräver en omfattande karta över dataläget och åtkomst ända ner till enhetsnivå.

Allt eftersom hotet från cyberbrott ökar för varje år, är absolut säkerhet en växande utmaning.



Tekniska utmaningar för efterlevnad



Hålla koll på enheter

Att uppfylla reglerna för dataportabilitet och rätten att bli bortglömd kräver en detaljerad redogörelse för alla personuppgifter som innehas av organisationen.

Vad du behöver känna till:

- Alla enheter som innehåller personuppgifter
- Alla enheter som har åtkomst till personuppgifter

Detta är det enda sättet att garantera att du kan hämta och/eller radera personuppgifter som innehas av företaget.

Hålla reda på moln

Det genomsnittliga europeiska företaget använder 608 appar, en siffra som uppskattas vara underrapporterad till 90 %. Anställda använder ofta kommersiella molnbaserade appar utan IT-avdelningens kännedom.[4]

För GDPR-efterlevnad måste moln begränsas till tjänster som är:

- Inom EU, och därför själva omfattas av reglerna för GDPR-efterlevnad
- Under jurisdiktion av en dataskyddsförordning som anses vara ”adekvat” av EU

Allt annat kan vara en överträdelse av internationella överföringsregler. Och du behöver veta vilka molntjänster den anställda använder om rätten att glömmas åberopas.

Hålla data skyddade

Hotet från cyberbrottslighet ökar. Inte minst för att även användningen av osäkrade nätverk och personliga enheter tilltar.

Överträdelser är nästan oundvikliga. EU känner till detta. Men för att undvika höga böter måste du:

- Implementera ett incidentövervakningsverktyg (SIEM) för att rapportera överträdelser inom 72 timmar
- Implementera klientsäkerhet i flera lager för att uppvisa vederbörlig omsorg i att förhindra överträdelser

Användare måste också vara medvetna om sitt ansvar och inte använda enheter och nätverk som inte godkänts.

[4]https://www.cloudindustryforum.org/content/cloud-and-eu-gdpr-six-steps-compliance

Hotet från cyberbrottslighet

Hotet från cyberbrottslighet är ett verkligt hot som bara ökar

82 %

av organisationerna har upplevt cyberhot/överträdelse de senaste 12 månaderna[5]

80 %

av IT-experterna anser att cyberbrottsligheten kommer att öka under de kommande tre åren[6]

78 %

av företagen rapporterar en ökning av attacker från skadliga programvaror under de senaste fem åren[7]

60 %

av IT-cheferna anser att cyberbrott är en utmaning för deras försvar[8]

81 %

av företagen uppskattar att intern oaktsamhet är det främsta hotet mot cybersäkerheten[9]

81 %

av IT-cheferna säger att mobila enheter på deras nätverk har varit mål för skadlig programvara[9]

72 %

anser att de anställdas användning av kommersiella molnbaserade program utgör en risk[9]

69 %

anser att egna enheter (BYOD) är en säkerhetsrisk

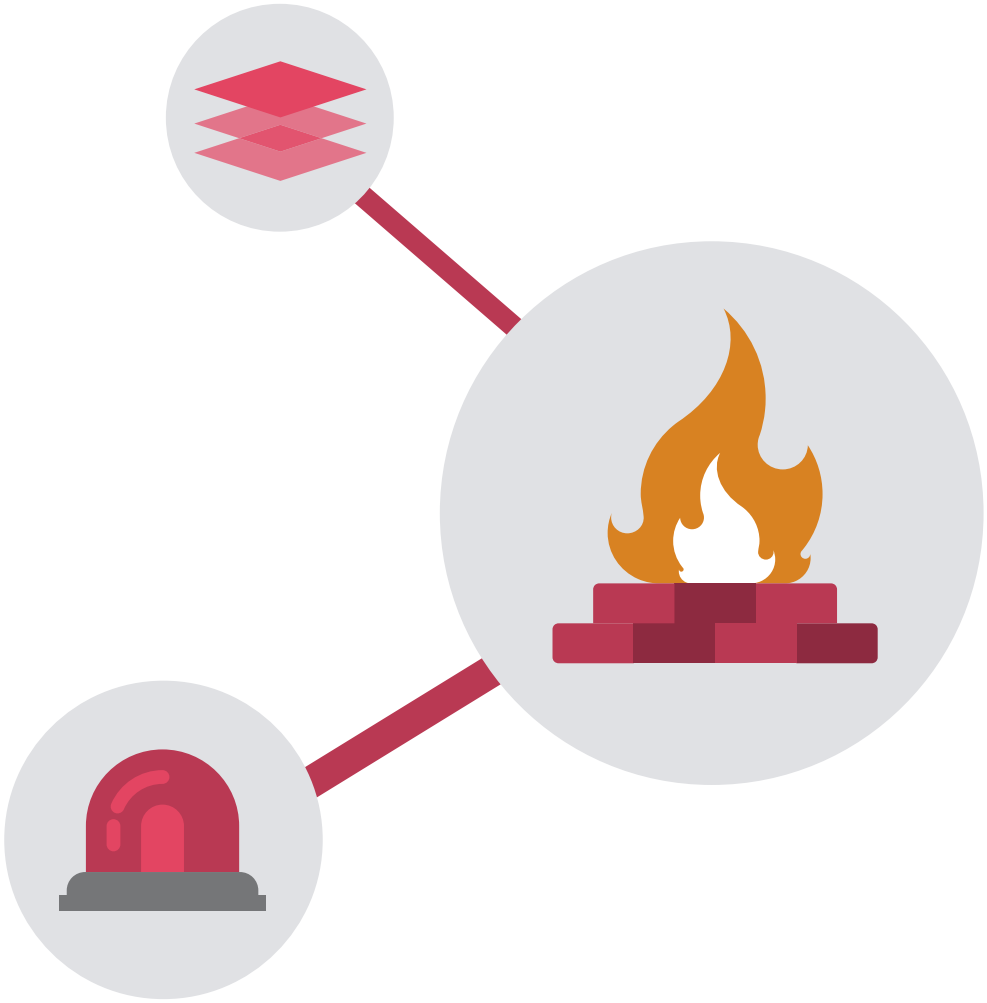
[5]HPI Printer Security Research 2016 (Spiceworks) [6]HP Printer Security Report 2015 [7] Ponemon 2016 State of the Endpoint Report [8]IBM CISO Assessment 2014 [9]Ponemon 2016 State of the Endpoint Report

Implementera klientsäkerhet

HPs flernivåstrategi för klientsäkerhet

En brandvägg och ett antivirusprogram är inte nog för att förebygga och skydda mot cyberintrång. Det har det aldrig varit. I en studie utförd av Damballa tog det antivirusprogrammet sex månader att identifiera och eliminera 100 % av de skadliga filer som det utsattes för.[10]

HPs uppfattning är att cybersäkerheten måste byggas i flera skikt och fungera på nätverks-, enhets- och användarnivå, med flera försvarsåtgärder på varje nivå. Att upptäcka och reagera bör föredras framför att skydda och försvara. Och klientenheterna är utgångspunkterna: både enheten och användaren.



Kritiska säkerhetskontroller (CSC)

Centret för internetsäkerhet (CIS) har definierat 20 internationellt erkända kritiska säkerhetskontroller (CSC) som utvecklats, förfinats och validerats av ledande IT-säkerhetsexperter runt om i världen. Dessa betraktas som viktiga näthygienåtgärder för alla organisationer.

Vi hänvisar till de viktigaste kritiska säkerhetskontrollerna för GDPR-efterlevnad eftersom de är användbara riktlinjer, men den fullständiga texten finns tillgänglig på nätet. Ladda ned den gratis från CIS library.

[10]https://www.damballa.com/time-to-fix-malware-strategies-2/

Nätverkssäkerhet

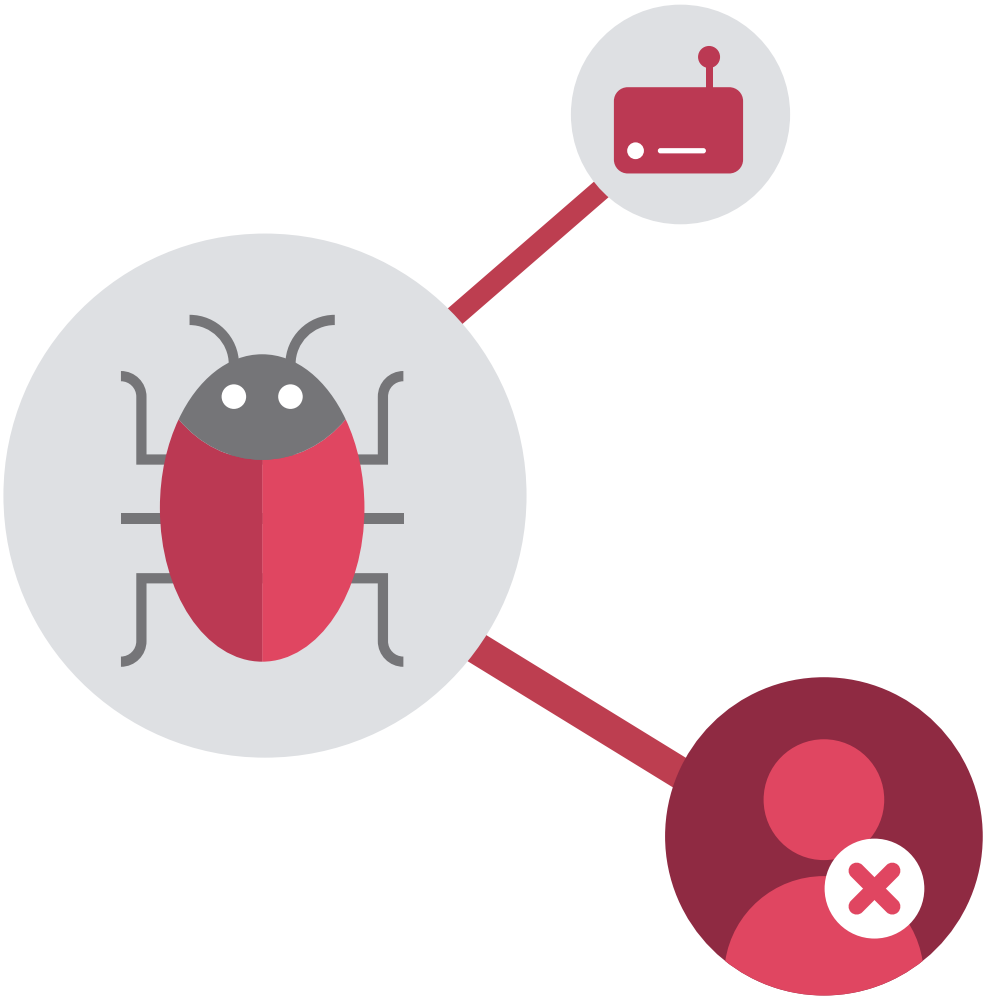
De stora hackarna tenderar att utnyttja en enda punkt för att få åtkomst till hela nätverket. Säkerheten på nätverksnivån bör därför baseras på att förebygga detta.

- **Kontrollera administrativa privilegier (CSC 5)**
  Begränsa rättigheterna att ändra nätverksinställningar och lösenord till så få personer som möjligt
- **Kontrollera åtkomst baserat på vad man behöver veta (CSC 14)**
  Separera åtkomst till känslig information om användare, enhet och plats. Väg säkerhetsrisk mot uppgifternas känslighet
- **Begränsning och kontroll av nätverksportar, protokoll och tjänster (CSC 9)**
  Stäng av onödiga åtkomstpunkter – såväl virtuella som fysiska – inklusive FTP, Telnet och utskriftstjänster
- **Underhåll, övervakning och analys av granskningsloggar (CSC 6)**
  Granska regelbundet revisionsloggar för att analysera systembeteende och upptäcka eventuell misstänkt aktivitet
- **Kontinuerlig sårbarhetsanalys och åtgärder (CSC 4)**
  Utför kontinuerliga miljöanalyser beträffande sårbarheter, vidta lämpliga åtgärder för att minimera riskerna för dataintrång

Målet är ett nätverk som delas upp enligt informationens känslighet. Åtkomstförfrågan utvärderas utifrån säkerhetsrisk. Okända enheter, användare och förfrågningar från osäkrade nätverk blockeras från den mest känsliga informationen. Googles BeyondCorp-policy är en bra modell.[11]

[11]https://research.google.com/pubs/pub43231.html

Nätverkssäkerhet



Varje enhet är en potentiell sårbarhet, vare sig den ägs av företaget eller är personlig. Du måste känna till alla telefoner, plattor, bärbara och stationära datorer som har tillgång till företagsdata.

- **Gör en förteckning över behöriga och obehöriga enheter (CSC 1)**
  Granska alla enheter som har åtkomst till data
- **Gör en förteckning över behörig och obehörig programvara (CSC 2)**
  Granska alla tillämpningar som används i nätverket – för direkt åtkomst till data eller ej
- **Försvar mot skadliga programvaror (CSC 8)**
  Se till att varje enhet har uppdaterade programvaror mot virus och skadliga program. Säkerställ regelbundna genomsökningar och uppdateringar

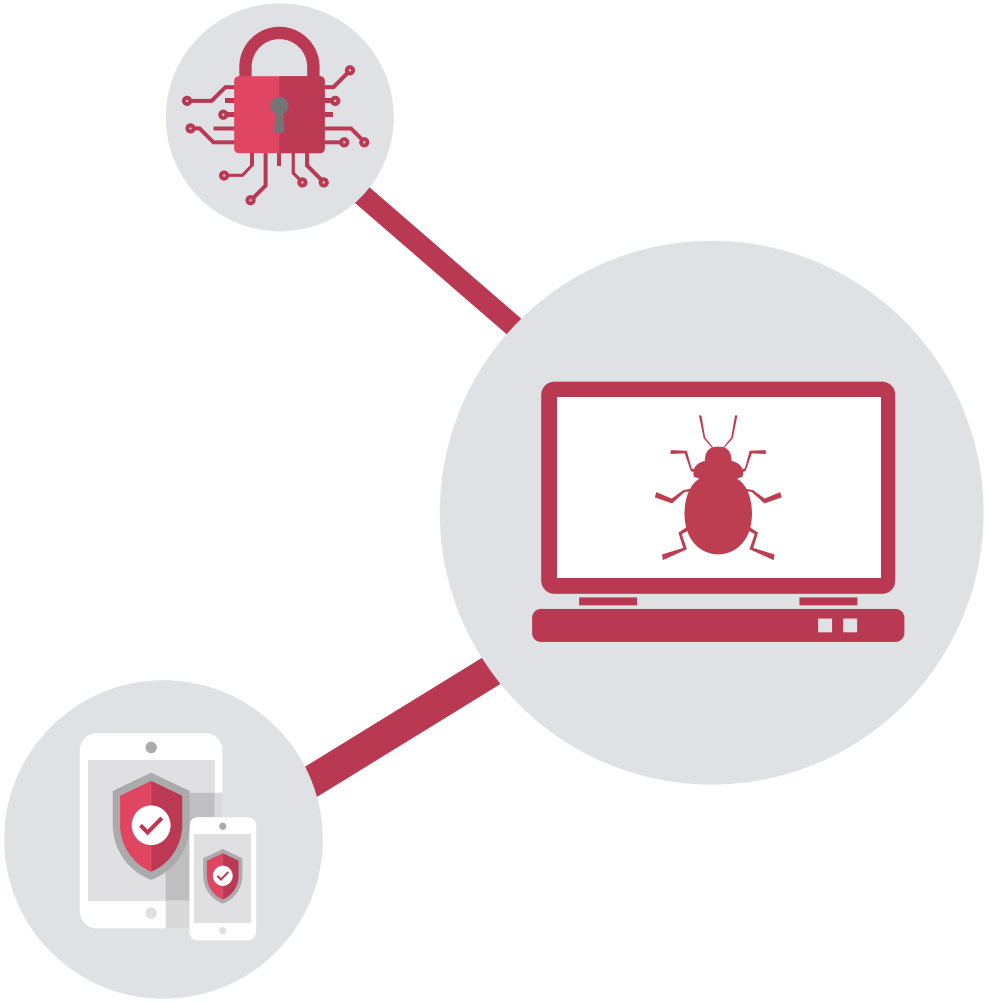
Enhetssäkerhet

Dessutom bör IT-avdelningarna överväga följande ytterligare kontroller:

- **Multifaktorautentisering**
  Se till att all arbetsutrustning är skyddad. Använd helst biometrisk autentisering tillsammans med lösenord (se sidan 14: ”Enheter med inbyggd integritet”)
- **Fjärråtkomst**
  Säkerställ att fjärråtkomst är möjlig till enheten för att hämta eller radera personuppgifter, isolera och avsluta processer, och stänga av och låsa enheten vid förlust eller stöld (se sidan 14: ”Upptäcka och reagera”)
- **Informera alla anställda om säkerhetsprotokoll och rutiner**
  Se till att alla anställda är medvetna om och känner till sitt ansvar när det gäller cybersäkerhet, inklusive att rapportera misstänkt aktivitet
- **Tillhandahåll aktiv cybersäkerhetsutbildning**
  Organisera workshops, seminarier, nätfiskeövningar – se till att alla vet hur man undviker grundläggande misstag och hur man uppfyller GDPR-kraven
- **Minimera användningen av egna enheter och appar**
  Motverka användning av personliga enheter och program för arbetsrelaterade uppgifter. En omfattande och flexibel CYOD-policy kan underlätta

Att implementera ett säkerhetsramverk som detta kommer att hjälpa dig att behålla kontrollen över företagsenheter för att skydda data och underlätta genomförandet av dataportabilitet och rätten att bli bortglömd.

För mer om HPs flerskiktiga säkerhetsstrategi, läs vår vitbok Säkerhet börjar med klientenheten (Security Begins at the Endpoint).



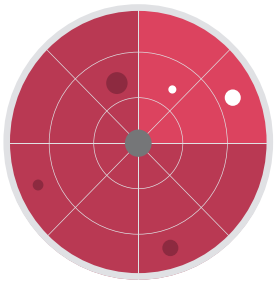
Varför varje anställd måste vara cybermedveten

58 % av cyberhoten kommer från anställda, tidigare anställda och betrodda partners. Att säkra varje enhet betyder att du även måste säkra användaren.

- Democratic National Committee (DNC) hackades 2016 när John Podesta klickade på en phishinglänk som felaktigt flaggats som legitim av en assistent[13]
- Kändisnakenbilder översvämmade internet 2014 när 36-årige Ryan Collins fick åtkomst till Jennifer Lawrences *m.fl.* iClouds genom att skicka enkla phishingmail där han utgav sig för att vara Apple[14]
- 68 miljoner Dropbox-lösenord läckte ut 2012 till följd av att en anställd använt samma lösenord för de interna systemen som för sitt LinkedIn-konto[15]
- President Donald Trump fortsätter att använda en vanlig Samsung Galaxy-telefon. Experterna undrar inte om den har hackats, utan snarare hur många utländska underrättelsetjänster som redan har gjort det[16]

[12]http://www.clearswift.com/sites/default/files/images/blog/enemy-within.pdf [13]https://www.theguardian.com/us-news/2016/dec/14/dnc-hillary-clinton-emails-hacked-russia-aide-typo-investigation-finds [14]http://www.forbes.com/sites/thomasbrewster/2016/03/16/icloud-hacking-jennifer-lawrence-fappening-apple-nude-photo-leaks/#45fed5d77b88 [15]https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach [16]https://www.theguardian.com/commentisfree/2017/feb/19/if-trump-hates-leaks-needs-to-give-up-phone

Upptäcka och reagera

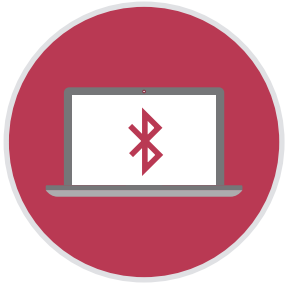


Upptäcka och reagera är ett cybersäkerhetssystem som utgår ifrån att totalt förebyggande är praktiskt omöjligt.

Det som är viktigt är att bli medveten om intrånget (upptäcka) och omedelbart vidta åtgärder (reagera).

Det finns programvara som gör varje enhet till en realtidssensor, vilket gör det möjligt för administratören att svara genom att t.ex. stänga av enheter, isolera filer och radera data.

Enheter med inbyggd integritet



HPs enheter materialiserar inbyggd integritet.

Säkerhetsfunktionerna omfattar världens första självläkande BIOS, automatiskt Bluetooth-lås som låser enheten när du går ifrån den, och integrerade sekretesskärmar.

Dessa funktioner garanterar inte i sig GDPR-efterlevnaden, men de hjälper definitivt till.

Att förbereda sig för GDPR

Praktiska steg att ta redan nu

GDPR träder i kraft den 25 maj 2018. Du har fortfarande tid på dig, men som du vet finns det mycket att göra.

Det första steget är att **granska den aktuella datasituationen**. Utvärdera var dina uppgifter lagras, vart de kopieras till och vem som har åtkomst till dem. Om du använder molnlösningar, ta reda på var deras servrar är baserade och om de uppfyller GDPR-kraven. Detsamma gäller för SaaS eller andra partnerorganisationer du samarbetar och delar dina uppgifter med. Detta kommer att ge dig en klar uppfattning om vilka ändringar som krävs för att uppfylla kraven.

Sammanställ en datapolicy. Inkludera detaljerade rutiner och protokoll om var uppgifter lagras, vem som har åtkomst till dem och kopior som skickas utanför företaget eller till andra länder i en multinationell organisation. Inkludera rutiner för att hämta och radera personuppgifter. Förmedla detta till alla i företaget. Anordna utbildningar. Understryk hur viktigt det är.

Sammanställ en säkerhetspolicy. Skapa ett nytt ramverk för cybersäkerhet som fungerar enligt principen ”upptäcka och reagera” vid klientenheterna. Uppdatera enhetspolicyn om det behövs. Investera i ny teknologi om det behövs. Endast 36 % av IT-cheferna anser att de har en tillräcklig budget för klientsäkerhet. GDPR-påföljder kan bli en kostsam varning som får ledningen att bli intresserad.

[17]Ponemon 2016 State of the Endpoint Report

Att förbereda sig för GDPR

Checklista för GDPR

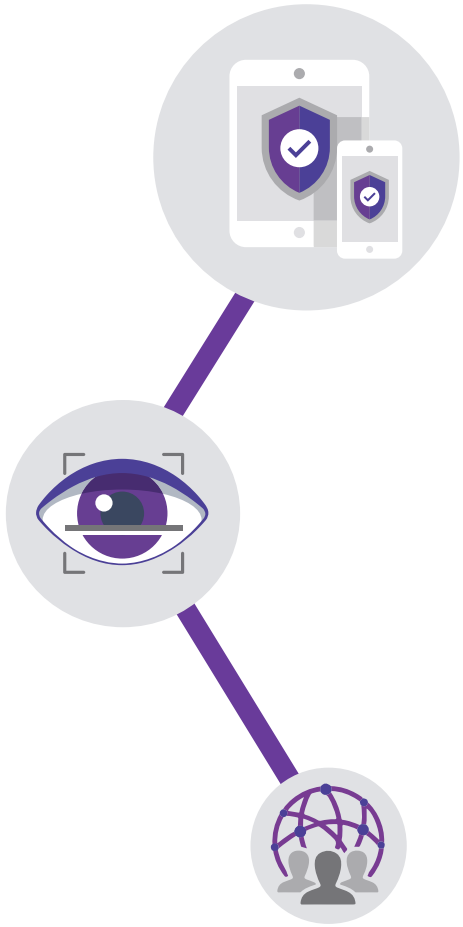
5 viktiga steg till GDPR-efterlevnad

1. Utse en person att ansvara för data, en Data Protection Officer (DPO) om det behövs
2. Utför en fullständig datagranskning, inklusive moln- och SaaS-leverantörers lämplighet avseende GDPR
3. Skapa ett nytt ramverk för datastyrning, inklusive rutiner för dataportabilitet och rätten att bli bortglömd
4. Skapa ett nytt ramverk för cybersäkerhet och implementera klientsäkerhet i flera skikt
5. Förmedla policyer och protokoll till alla i företaget

Checklista för säkra enheter

6 viktiga steg för att säkra klienter

1. Granska alla auktoriserade och icke-auktoriserade enheter med åtkomst till personuppgifter
2. Investera i nya, säkrare enheter om nödvändigt
3. Säkerställ fjärråtkomst och raderingsrättigheter för företagsdata på enheter
4. Inför en policy för regelbundna genomsökningar och uppdateringar av säkerhetsprogram
5. Inför realtidsdetektering och responsprogramvara
6. Utbilda de anställda om cybersäkerhet



Klientsäkerhetskalender

En grundläggande tidsplan för implementering av klientsäkerhet genom GDPR

2017

Maj

Utse en projektledare med ansvar för att genomföra klientsäkerhet

Juni

Utför en granskning av nuvarande säkerhetspolicy, rutiner och enheter

Juli

Överväg enhetskrav och policy för klientsäkerhet (CYOD/BYOD etc.)

Augusti

Överväg programvarulösningar för att upptäcka och svara på säkerhetshot

September

Upprätta differentierad åtkomst till företagsdata i flera skikt

Oktober

Utforma offentliga/privata moln för att möjliggöra lämplig extern dataåtkomst

November

Utforma användarutbildningar inkl. regelbundna nätfiskeövningar

December

Förmedla nya säkerhetspolicyer till resten av företaget

2018

Januari

Implementera ny dataarkitektur på offentliga/privata moln

Februari

Implementera en ny enhetspolicy

Mars

Implementera en programvarulösning för att upptäcka och reagera

April

Genomför användarsäkerhetsutbildning inkl. policyer relaterade till GDPR

Maj

GDPR träder i kraft

Sammanfattning

GDPR är inte långt borta

I bästa fall gör din organisation redan mycket av vad som står i förordningarna – de är i huvudsak en sammanfattning av vad som redan utgör bästa praxis.

Och om du har varit verksam i flera EU-länder har du kanske redan stött på några av de mer stränga åtgärderna i förordningen.

De säkerhetsåtgärder som vi rekommenderar att införa i syfte att följa GDPR är åtgärder som bidrar till att förhindra alla typer av överträdelser, som kan vara oerhört kostsamma för en organisation. Vid den senaste bedömningen uppskattade den brittiska regeringen att brittiska företag förlorat 21 miljarder pund på ett enda år, en siffra som förväntas växa.[18]

Vidare bidrar många av de åtgärder som krävs för en robust säkerhet också till att uppfylla andra aspekter av GDPR. Att begränsa datatillgängligheten till vissa användare, enheter och nätverk minimerar inte bara datarisken, det gör det enklare att spåra personuppgifter och därmed att uppfylla kraven för dataportabilitet och rätten att bli glömd, för att inte tala om internationella överföringar.

Denna e-guide är bara en början. Säkerhet har alltid varit en prioritet för HP. Inbyggd integritet är sedan länge vår policy. Nu när det blir ett krav snarare än en rekommendation är vi väl förberedda att hjälpa dig att anta samma strategi.

För att läsa mer om hur HP och hur våra produkter kan hjälpa dig med att efterleva GDPR, besök vår webbsida **”Inbyggd integritet” (Privacy by Design)**.

[18]https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the cost-of-cyber-crime-full-report.pdf