Onboarding:

Dataskydd

SECIFY

Innehållsförteckning

1. INFÖRANDET

Den här guiden medföljer videon för att ge råd till organisationer för att hjälpa personalen att uppfylla dataskyddsskyldigheterna.

Dataskydd och integritet bör ligga i framkant av allas jobb inom organisationen - inbyggd och default bör vara en del av organisationskulturen så att anställda överväger effekterna av behandling av personuppgifter av vad de gör.

GDPR lägger en juridisk skyldighet på anställda lika mycket som en organisation, så det är viktigt för organisationer att se till att anställda är medvetna om sitt ansvar.

2. VAD SKA DE VETA?

2.1. DATASKYDDSOMBUD

Personalen ska veta vem som har ansvar för GDPR, dataskydd och integritet inom organisationen. Denna information bör vara lätt att hitta tillsammans med tydliga funktioner som dataskyddsombudet tillhandahåller, till exempel hantering av frågor eller överträdelser.

2.2. DATA RÄCKVIDD RAPORTERING & HANTERING

Företaget bör ha en tydlig process för rapportering av överträdelser och hantering av överträdelser. Personalen bör göras medveten om att överträdelser av personuppgifter måste rapporteras snarast eftersom det finns en tidsram för rapportering som anges i GDPR. Personalen bör förses med ett formulär för rapportering av överträdelser eller en tydlig struktur för att säkerställa att så mycket relevant information som möjligt tillhandahålls när de lämnar in rapporten. Detta minskar också den tid som krävs för ytterligare informationsinsamling eller förtydligande.

När organisationen tar emot en anmälan om intrång bör den ha en tydlig process för hantering av överträdelser. Någon måste bedöma om överträdelsen är mindre och bara

behöver registreras i ett intrångsregister eller om processen för att svara på överträdelser behöver initieras. Alla processer för att bemöta överträdelser måste inkludera dataskyddsombudet för att de ska kunna bedömarapporteringsskyldigheterna så tidigt i processen som möjligt.

Alla svar på överträdelser bör dokumenteras för att ta hänsyn till vidtagna åtgärder. Och organisationen kommer helst att göra en granskning i slutet av processen för att förbättra hanteringen av överträdelser.

2.3. HANTERING AV UPPGIFTER

Anställda bör få årlig dataskyddsutbildning för att hålla dem informerade och uppdaterade om GDPR-utvecklingen. Helst bör träning levereras i korta sessioner eftersom långa sessioner tenderar att vara mindre effektiva.

Anställda bör överväga vilka personuppgifter de hanterar och förstå de processer som finns för att säkerställa att personuppgifter hanteras korrekt. Organisationen bör klargöra att dessa processer är på plats på grund av de juridiska skyldigheter som GDPR ålägger företaget och de anställda.

2.4. DATAÖVERFÖRING OCH UTLÄMNANDE

Detta bör även omfatta processer och policyer för informationsutbyte och utlämnande. Organisationen bör avskräcka från delning av personlig information via e-post, särskilt om e-postmeddelandet inte är krypterat. Organisationen bör se till att personalen har tillgång till säkra överföringsmetoder om personuppgifter måste delas med externa personuppgiftsbiträden.

När de hanterar registrerade måste anställda förstå att de inte kan anta att personen de skickar e-post eller pratar med är den registrerade. En process bör utvecklas för att verifiera att personen är den registrerade eller har en fullmakt att agera på den registrerades vägnar.

Organisationen bör ha tydliga disciplinära förfaranden för obehöriga överföringar av personuppgifter, till exempel till personliga webbmailkonton eller overifierade registrerade.

2.5. GDPR-EFTERLEVNAD

Organisationer bör se till att anställda förstår de skyldigheter som GDPR ålägger dem när det gäller hur länge personuppgifter sparas, hur de använder dem och hur de tar bort dem.

Organisationen bör för personuppgifterna bedöma om uppgifterna är raderade, pseudonymiserade anonymiserade. Detta beror på systemet - till exempel kan databaser skadas om poster raderas, så att skriva över data för att anonymisera det är det normala tillvägagångssättet för att säkerställa att data "raderas".

3. SLUTSATS

Bra utbildning för alla anställda som hanterar personuppgifter som förmedlar sin rättsliga skyldighet på personlig nivå kommer att hjälpa organisationer med deras GDPR-efterlevnad.

Organisationer kan vidta ett antal tekniska åtgärder för att minimera riskerna för bristande efterlevnad, men i slutändan är det beroende av att personal som hanterar uppgifterna är medvetna om sitt ansvar och de processer som styr hanteringen.

Att se till att anställda är utbildade, är medvetna om processer och var de kan hitta vägledning och hjälp kommer att minska efterlevnadsriskerna.