De store GDPR faldgruber

Af Lars Abild
14. juni 2018 kl. 12:50

Helle Mering, indehaver af SOSY A/S.

Beskyt kundernes data. Det lyder så ligetil, men det kræver ifølge ekspert en helt ny tankegang at udføre det i praksis. Siden 1989 har Helle Mering arbejdet med softwareløsninger. Nu hjælper hun virksomheder med at identificere deres udfordringer med de nye persondataregler – og dernæst få løst dem. Kom med ned i maskinrummet, og hør ejeren af SOSY A/S fortælle om hendes lavpraktiske tilgang til beskyttelse af persondata.

Der er blevet strammet gevaldigt op på, hvordan man må udvikle digitale løsninger og hvilke data, man må bruge til udviklingen. Det sker blandt andet for at beskytte kundernes data, så de ikke ved et uheld ligger og flyder på nettet.

Det lyder så lige til, men det kræver en helt ny tankegang, siger Helle Mering, der har arbejdet med softwareløsninger siden 1989 og ejer virksomheden SOSY A/S.

Målet – at blive data compliant – er ikke det værste, man kan skilte med i disse år. Men det kræver sit at få styr på og dokumenteret sine processer, fortæller hun.

Men hvad er det rent lavpraktisk, der finder sted, når der skal styr på data, og hvordan løser man nogle at de helt åbenlyse udfordringer, som hidtil ikke er blevet taget synderligt alvorligt? Men som man nu kan få endog meget store bøder for, hvis det ikke er på plads?

Kotyme at kopiere produktionsdata
Helle Mering fortæller om en kendt problemstilling: Udvikling af produkter til ens digitale løsninger, som finder sted med en virksomheds produktionsdata.

”Selv om det aldrig har været god ’compliance- skik’, har det i mange år for mange virksomheder været kutyme, at man bare tager en kopi af produktionsdata og tester på dem. Det siger de nye persondataregler, at man ikke må, når der er tale om følsomme data, det vil sige personhenførbare data. Og med de store bøder, som man kan risikere med GDPR, bliver problemstillingen taget meget mere alvorligt nu.”

Konkret kan det være, at man er ansat i en HR afdeling, hvor man arbejder med løn og statistikker og den slags for medarbejdere. Det er sensitive data. Naturligvis har ansatte i afdelingen brug for disse data til at varetage deres job, men en kopi af disse data må ikke bare sendes videre til udviklingsafdelingen. Det skal ske med såkaldte testdata, og derfor bliver det at teste med data i en udviklingsproces en reel udfordring, når EU’s persondataforordning, GDPR, skal efterleves.

Dataintegritet er kommet på menuen
”En af de løsninger, vi tilbyder, er, at man automatisk kan anonymisere produktionsdata, når de skal bruges som testdata. Det betyder, at man kan teste på medarbejdere eller kunder, der har de samme karakteristika, men at udvikleren eller testeren ikke kan se, hvis data der er tale om,” siger Helle Mering.

Processen er så ifølge direktøren, at man finder ud af, hvilke data, man har, der er sensitive.

”Det er ikke alle, der er følsomme. Det er typisk kun visse kolonner eller rækker i databaserne. Dernæst skal man beslutte, hvordan man ønsker at anonymisere de følsomme data. Der findes forskellige former for pseudonymisering,” fortæller hun.

Når den fase i forløbet er på plads, er det naturligvis meget vigtigt, at de testdata, man får produceret, kan bruges til noget. Det kaldes at bevare ”dataintegriteten”.

Mickey Mouse må ikke blive Anders And
”Det sværeste i processen er at sikre, at ’dataintegriteten’ bevares for testdata. Det betyder, at den rigtige sammenhæng mellem de forskellige data bliver bevaret, så man eksempelvis kan teste et helt ordreforløb igennem. Det nytter jo ikke noget, hvis data i kundedatabasen anonymiseres på én måde, og kundedata i ordre-, fakturerings- og leveringsdatabaserne pseudonymiseres anderledes. Så kan man ikke finde et eksempel på et helt forløb at teste med.”

Den let forståelige version er, at hvis kunden eksempelvis får pseudonymet Mickey Mouse et sted, så skal Mickey Mouse også være at finde de andre steder. Så kan man teste hele forløbet, og det er nødvendigt for at sikre, at alle delfunktioner og delprocesser fungerer i et længere forløb. Anonymiseringen betyder samtidig, at man kan vise, at man overholder GDPR-forordningen, hvis eksempelvis Datatilsynet gerne vil kontrollere det.

Helle Mering fortæller, at der er alt for mange skrækkelige eksempler på, at man bare har testet på produktionsdata. Hvis der så kommer et læk af dem, når man vil se om det, man har udviklet, virker, så er der problemer. Nu er GDPR-forordningen trådt i kraft, og det drejer skruen endnu en omgang.

”Hvis ens testdata er ordentlig anonymiserede, er det jo ikke længere følsomme data. Derfor bliver en eventuel læk ikke problematisk og kritisk på samme måde. Og det er jo netop et af hovedformålene med GDPR, at følsomme data bliver beskyttede.”

Få styr på Slaraffenland
Et af de forhold, der ofte bliver nævnt i forbindelse med GDPR er, om man har styr på, hvem der har adgang til ens systemer og dermed til databaserne, og hvad brugerne så laver, når de er logget på.

”Mange virksomheder ved ikke, hvad folk laver, når de arbejder på systemet. Det gælder både for interne medarbejdere og eksterne konsulenter. Må folk lave det, de gør, og hvilke data har de adgang til? Mange gange tror de dataansvarlige, at der er godt styr på det, men min erfaring siger mig, at det ofte ikke er tilfældet,” lyder det fra Helle Mering.

Det kan virke utroligt simpelt, men en af de fejl, der ofte bliver begået, er adgangen til systemet. Når der kommer en ny medarbejder, så kopierer man en brugerprofil fra en ansat i samme afdeling. Det er nemt og hurtigt, men også problematisk.

”Er man nu sikker på, at det er en selvfølge, at den pågældende skal have adgang til alle de samme databaser og menupunkter, som den man har kopieret brugerprofilen fra? Det kan hurtigt blive noget værre rod i forhold til GDPR, at der bare er blevet kopieret fra samme brugerprofil til den næste og den næste og så videre. Virksomhederne skal i dag have styr på, hvad den enkelte bruger af systemerne må og kan, når han eller hun er logget på,” siger hun.

Dokumentation er stor akilleshæl
Reglerne stiller også krav om, at man skal kunne dokumentere væsentlige arbejdsprocesser i virksomheden i forhold til de nye regler for at finde ud af, om man er compliant. Det kan være lige nøjagtig så kedeligt og tidskrævende, som det lyder, når man skal tage skærmprints af arbejdsgange og kopiere det over i Word eller PowerPoint. Få de rigtige kommentarer med instrukser med. Men det er nødvendigt blandt andet for at kunne oplære nye kolleger.

”Vi tilbyder en løsning, der automatisk dokumenterer alt, hvad man gør, man kan indsætte kommentarer undervejs eller senere, og resultaterne kan konverteres til Word/PDF eller animationsfilm, som ofte er populære til undervisningsbrug,” siger Helle Mering.

Retten til at blive glemt
En af de nye rettigheder, en kunde har, er at bede om at blive slettet. Det kræver, at virksomheden ved, hvilke data man har på den enkelte kunde, hvilke databaser de ligger i, og at man har en klar procedure for, hvordan man let og hurtigt kan slette dem.

”Derved bliver det ikke kun virksomhedens data protection officer, der skal have styr på de følsomme data. De kolleger, som skal udføre processerne, skal også vide det, og dokumentationen skal være ajour,” siger Helle Mering.

Helle Mering
Helle Mering har siden 1989 arbejdet med SOSY’s softwareløsninger og udført konsulentarbejde. Oprindeligt var det primære fokus system management området, men siden er et antal nye forretningsområder kommet til. I dag er de primære områder for SOSY A/S løsninger til software test, sikkerhed og realtidsdatareplikering. Hun har gennem årene holdt

mange indlæg om SOSY's forretningsområder og software løsninger på konferencer i ind- og udland. Hun overtog virksomheden i SOSY A/S i 2003.

Skrevet af

Lars Abild, Journalist

Ansættelser på hhv. Børsen, Jyllands-Posten og Berlingske. Har endvidere arbejdet freelance med fokus på dokumentarudsendelser for DR og TV2. Skrevet artikler til Information, Weekendavisen og Økonomisk Ugebrev.