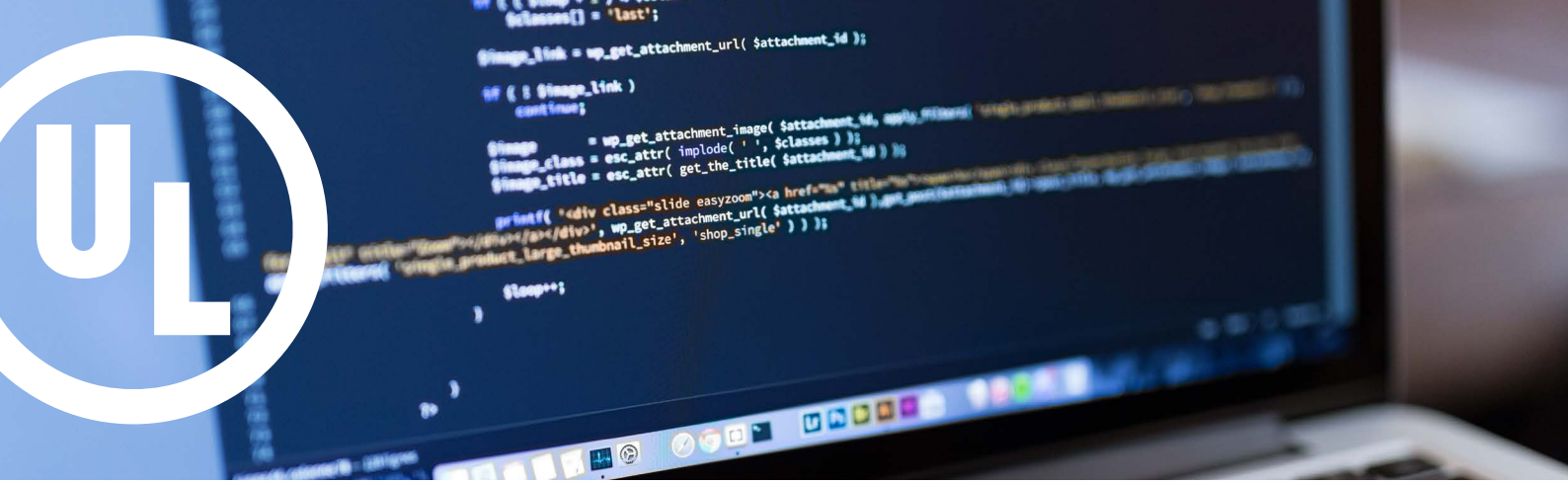

UL'S PRIVACY SERVICES

Bescherming Persoonsgegevens

Er is een toenemende trend van automatisering, digitalisering, en meer analyse en gebruik van data als onderdeel van cloud computing, mobiele communicatie, sociale media etc. Hoe meer diensten, data, en informatie worden gedigitaliseerd en geïntegreerd in digitale toepassingen - toegankelijk via het internet of interne netwerken - hoe groter bepaalde privacy risico's. Wereldwijd zijn er steeds meer (cyber)incidenten (waaronder datalekken) met digitale netwerken en systemen waarbij de schade voor organisaties steeds hoger oploopt. Regelgeving speelt op deze risico's in. De Nederlandse Wet bescherming persoonsgegevens benadrukt het belang van adequate privacybescherming. Begin 2018 wordt deze wet vervangen door de Europese Algemene Verordening Gegevensbescherming, waarbij de privacybescherming, en de boetes bij niet-naleving, nog hoger worden.

- Bent u ervan op de hoogte welke privacygevoelige gegevens uw organisatie verzamelt of gebruikt?
- Weet u wat de schade kan zijn als privacygevoelige gegevens verloren gaan, of in handen vallen van een cybercrimineel?
- Weet u wat uw wettelijke verplichtingen zijn en wat u moet doen om deze na te leven, zoals het melden van datalekken? [1]

Wat houdt dit precies in?

Elke organisatie dient persoonsgegevens zorgvuldig te verzamelen en te gebruiken, in overstemming met wettelijke regels en verplichtingen. De verantwoordelijkheid hiervoor ligt bij de organisatie – ook als een incident plaatsvindt bij een derde organisatie, zoals een cloud- of hostingprovider.

Van organisaties wordt verwacht dat ze bij ontwikkeling en toepassing van (nieuwe) technologieën, diensten en producten, privacy risico's inschatten en mitigeren. Een activiteit zoals 'privacy-by-design', het inbouwen van privacy verhogende maartegelen in een vroeg stadium, kan hieraan bijdragen.

Een andere belangrijke activiteit, in steeds meer gevallen zelfs verplicht,[2] is een privacy impact assessment (PIA). Een PIA betreft een inschatting van privacy risico's en impact. Met dit inzicht kunnen tijdig maatregelen worden genomen om privacy risico's te bestrijden.

Welk nut heeft dit voor mijn organisatie?

Een groeiend aantal incidenten draagt eraan bij dat consumenten steeds alerter worden op het gebruik van hun persoonlijke gegevens. Een data- of veiligheidslek kan grote financiële en reputationele gevolgen met zich meebrengen.

Zonder inzicht in privacy risico's en het tijdig nemen van maatregelen loopt uw organisatie mogelijk grote schade op, bijvoorbeeld door het achteraf moeten invoeren van aanpassingen in systemen en projecten. Bovendien gelden wettelijke verplichtingen, en bij niet-naleving daarvan, hoge administratieve boetes.

Privacy Impact Assessment

Een gezonde balans vinden tussen het gebruik van persoonsgegeves en privacy bescherming is een grote uitdaging. UL helpt bij het in kaart brengen van privacy-impact en risico middels een PIA. Dit begint met het beoordelen van de impact van een nieuw systeem of product, door te kijken naar welke data er worden verzameld en gebruikt, waar data zich bevinden en wie toegang heeft tot data, etc.

UL integreert bestaande PIA modellen, zoals van NOREA, SURFnet en het PIA toetsmodel van de Rijksoverheid, in een pragmatische

---

[1] Vanaf 1 januari geldt een wijziging in de Wbp, ook wel de Meldplicht Datalekken genoemd. Dit brengt voor organisaties een verplichting met zich mee om datalekken onmiddellijk te melden en te beheersen.

[2] Het regeerakkoord introduceert een verplichte PIA voor overheden. De Europese Algemene Verordening Gegevensbescherming zal PIA's voor zowel overheden als private organisaties verplicht stellen.

aanpak, waarbij we alle relevante privacy wettelijke verplichtingen, principes, en maatregelen in overweging nemen.

UL evalueert onder andere het doel van gegevensverbruik, databeveiligingsniveaus en -maatregelen, en mogelijkheden tot limitering van gegevensverbruik. Vervolgends adviseert UL welke aanvullende maatregelen er kunnen worden getroffen, zoals bijvoorbeeld toegangscontrole tot data.

UL brengt diepe technische informatiebeveiligingsexpertise met zich mee. UL kan gedetailleerd inzicht verschaffen in beveiligingsmaatregelen zoals identificatie-, authenticatie- en autorisatieprocessen en encryptie (waaronder PKI encryptie) en tokenisatie.

Compliance Check

Op het gebied van privacy en security geldt een ingewikkeld geheel van strikte wettelijke (privacy) regels. Sinds 1 januari 2016 is de boete voor het niet naleven van deze verplichtingen verhoogd tot €810.000. Begin 2018 treedt de Algemene Verordening Gegevensbescherming in werking, en worden de boetes nog hoger en wijzigen de verplichtingen.

Om aan de meldplicht datalekken te voldoen en vooruit te lopen op de invoering van de Algemene Verordening Gegevensbescherming, biedt UL in samenwerking met De CLERCQ Advocaten Notarissen de Compliance Check aan. De CLERCQ is een middelgroot advocatenkantoor waar het gespecialiseerde Tech, Data & Innovation-team zich onder andere richt op privacy- en securityvraagstukken.

De Compliance Check bestaat uit:

- Juridische analyse van de verwerkte (persoons)gegevens;
- Juridische analyse van de betrokken (sub-)bewerkers;
- Opstellen en afsluiten van (wettelijke verplichte) bewerkersovereenkomsten;
- Opstellen van een protocol meldplicht datalekken en/of een beleid verwerking persoonsgegevens.

Case Study: Privacy Impact Assessment voor Europese Bank

Achtergrond: The organisatie moest een PIA uitvoeren in verband met de introductie van nieuwe mobiele betaaltechnologie (Host Card Emulation (HCE)-technologie), gebruikmakend van een applicatie gekoppeld aan een cloud server.

Dienstverlening: UL ontwikkelde een strategie met aandacht voor de beveiliging van data, door in de eerste plaats inzichtelijk te maken waar data worden opgeslagen dan wel gecommuniceerd, en wie er toegang tot de data heeft. UL adviseerde over het implementeren van beveiligingsmaatrelen om privacygevoelige data beter te beschermen.

Resultaat: De organisatie had een inzichtelijke PIA tot hun beschikking en kon op basis daarvan de juiste doeltreffende maatregelen nemen, wat resulteerde in een succesvolle uitrol van de mobiele betaaltechnologie.

Wat zijn voordelen van het werken met UL?

- Expertise: Security & privacy industrie leider, met diep inzicht in en kennis van informatiebeveiliging.
- Onafhankelijk: Neutraal, derde partij, privacy onderzoek, met concrete aanbevelingen voor het mitigeren van risico's
- Continuïteit: Herevaluatie en support, bij het invoeren van nieuwe systemen en technologie, dan wel als nieuwe risico's aan het licht komen.

DE CLERCQ Advocaten · Notarissen

CONTACT

ulcyber@ul.com

ul.com