TRUST IN GERMAN SICHERHEIT

G DATA Whitepaper

De nieuwe algemene EU-verordening voor gegevensbescherming – Wat ondernemingen absoluut moeten weten

G DATA Software AG | September 2017

Inleiding

Gegevensbescherming is meer dan een verplicht nummer. De vernieuwde algemene EU-verordening voor gegevensbescherming (EU-AVG) plaatst het thema nu in heel Europa op de agenda. Vóór 25 mei 2018 moeten ondernemingen zich aanpassen aan de nieuwe rechtspositie en de gegevens van hun klanten doeltreffend beschermen. Er zijn hoge straffen voor het niet naleven van de nieuwe verordening en er gelden overeenkomstige strenge maatregelen. Medewerkers moeten worden geïnformeerd en workflows en tools gecontroleerd om te garanderen dat klantgegevens conform de wet worden verwerkt. Ook op het vlak van IT moet een aanzienlijk aantal maatregelen worden getroffen. In deze whitepaper vindt u de belangrijkste vereisten van de verordening voor gegevensbescherming. U ontdekt ook hoe een totaaloplossing voor IT-beveiliging u kan helpen bij het voldoen aan deze vereisten.

1. Wat is de EU-verordening voor gegevensbescherming?

De EU-verordening voor privacy-wetgeving (EU-AVG) werd in april 2016 aangenomen door het Europese parlement en regelt de modernisering en de standaardisering van de privacywetgeving voor heel Europa. Het doel hiervan is de bescherming van persoonlijke gegevens te garanderen, rekening houdend met de volgende beginselen[1]:

- Rechtmatigheid, verwerking te goeder trouw, transparantie
- Doelbinding
- Gegevensminimalisering
- Correctheid
- Opslagpositie
- Integriteit en vertrouwelijkheid

De verordening vervangt de verouderde Data Protection Directive (DPD) van 1995. In tegenstelling tot de DPD is de EU-AVG niet “gewoon” een richtlijn, maar een echte wet. Dit betekent dat de verordening niet los van de EU-lidstaten moet worden geïmplementeerd. Daarom is dit al sinds 24 mei 2016 van kracht. Om bedrijven de tijd te geven zich aan de nieuwe wetgeving aan te passen, werd een overgangstermijn tot en met 25 mei 2018 voorzien. Tot deze datum hebben ondernemingen de tijd, de bepalingen van de EU-AVG in de praktijk om te zetten. Als dat niet gebeurt, kunnen hoge boeten worden opgelegd.

2. Op welke ondernemingen is de EU-AVG van toepassing?

De verordening voor gegevensbescherming regelt de bescherming van persoonsgegevens. Daarom zijn alle ondernemingen die persoonsgegevens van privépersonen verwerken, hierbij betrokken. Om duidelijk te maken op welke gegevens de wet betrekking heeft, is de volgende definitie opgenomen in artikel 4 van de wettekst:

[1] Artikel 5 van EU-AVG. De complete wettekst vindt u onder http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679.

Copyright © 2017 G DATA Software AG

“Overeenkomstig deze verordening verstaan we onder “persoonsgegevens”, alle informatie die betrekking heeft op een geïdentificeerde of identificeerbare natuurlijke persoon; als identificeerbaar wordt beschouwd, een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatie, zoals een naam, een identificatienummer, locatiegegevens, een online id of een of meer specifieke elementen die kenmerkend zijn voor zijn/haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit”.
De definitie is dus zeer ruim. Typische gegevens die door de onderneming worden verzameld en door de EU-AVG worden beschermd, zijn de naam, het adres, het e-mailadres of het IP-adres. In de bedrijfscontext gaat het dan vaak om de klantgegevens die bijvoorbeeld in een CRM-systeem worden verwerkt. Maar ook gegevens die alleen voor marketingdoeleinden worden gebruikt of als “bijvangst” worden geregistreerd, zoals een IP-adres in een logboekbestand, worden door de EU-AVG beschermd.

3. Welke rechten hebben klanten in de EU-AVG?

De EU-AVG beschrijft de bepalingen die ondernemingen in de praktijk moeten omzetten als ze persoonsgegevens verwerken. Hoewel veel maatregelen al in de Data Protection Directive zijn gedefinieerd, zijn er enkele nieuwe bepalingen die zelfs voor bedrijven die tot nog toe altijd “compliant” waren, een werkelijke uitdaging zullen betekenen. Een kort overzicht:

- Recht om te worden vergeten: klanten hebben “het recht te verlangen dat hun persoonsgegevens worden verwijderd” (artikel 17).
- Doelbinding en het goedkeuringsrecht: dit is al voor een deel vastgesteld in de wet op de bescherming van persoonsgegevens, maar wordt in de EU-AVG verduidelijkt. Elke klant moet “uitgebreid en in klare taal” over de gebruiksdoeleinden van gegevens worden geïnformeerd. De toestemming voor het gebruik moet vrijwillig gebeuren. Deze mag dus niet worden gekoppeld aan andere voorwaarden (zoals het toestaan van het commerciële gebruik van de gegevens om een bestelling te kunnen afsluiten); dit is vastgelegd in overwegingen 42 en 43 van de EU-AVG.
- Snelle melding aan de toezichthoudende autoriteit: “In het geval van een inbreuk op de beveiliging, meldt de verantwoordelijke dit onmiddellijk en indien mogelijk binnen 72 uur nadat hij/zij de inbreuk heeft ontdekt, aan de toezichthoudende autoriteit” (Artikel 33).
- Recht op gegevensoverdraagbaarheid: Klanten hebben het recht de over hen opgeslagen gegevens “in een gestructureerd, gangbaar en door een machine leesbaar formaat te ontvangen” (artikel 20).

Het is duidelijk dat de toepassing van deze rechten en hun voorstelling in de bedrijfsprocessen niet triviaal zijn. Zo vereisen veel bepalingen dat ondernemingen weten in welke omvang en op welke locaties persoonsgegevens zijn opgeslagen. Dat kan nog van toepassing zijn in een klein bedrijf met slechts één centrale klantendatabase. Maar bij het bekijken van gegevensbronnen, zoals videobewaking in openbare ruimten of bij de verwerking van gegevens op cloud-platforms (zoals Salesforce), wordt het duidelijk dat veel bedrijven veel meer persoonsgegevens opslaan en verwerken dan ze zich echt bewust zijn. Deze gegevens worden ook buiten het bereik van de eigen directe invloed opgeslagen of verwerkt. Het is ook mogelijk dat er conflicten ontstaan wanneer een klant gegevens wil laten verwijderen, maar deze in het kader van andere wetten moeten worden bewaard (zoals factuurgegevens).

4. Wat gebeurt er bij inbreuken op de EU-AVG?

Niet alleen de in de EU-AVG beschreven maatregelen zijn nieuw. Ook de boeten voor ondernemingen die deze maatregelen niet of onvoldoende toepassen, zijn opnieuw gedefinieerd. Als een gegevensbeschermingsautoriteit een inbreuk vaststelt, kunnen de volgende geldboeten worden opgelegd, afhankelijk van de ernst van een geval:

- Tot € 20 miljoen euro of 4 % van de wereldwijde jaaromzet van het bedrijf (het hoogste bedrag wordt toegepast)
- Tot € 10 miljoen euro of 2 % van de wereldwijde jaaromzet van het bedrijf (het hoogste bedrag wordt toegepast)

De eerste boetecategorie wordt bijvoorbeeld gebruikt wanneer een onderneming een inbreuk pleegt op de bepalingen in artikel 17 (recht om vergeten te worden). De laatste categorie is voorzien voor verhoudingsgewijs kleine inbreuken, zoals het niet naleven van de meldingsplicht conform artikel 33, maar kan echter bij een maximumbedrag van € 10 miljoen euro of 2 % van de omzet nog steeds zeer hoog uitvallen. De geldboeten zijn gedefinieerd in artikel 83 van de EU-AVG waarin ook wordt gegarandeerd dat het opleggen van geldboeten in elk geval “doeltreffend, evenredig en afschrikkend” is. De nationale wetgeving van indivuduele EU-lidstaten kan dit nog versterken, in Duitsland bv. is ook de aansprakelijkheid veranderd sinds de inwerkingtreding van de EU-AVG: in artikels 41 tot 43 van de wet op de aanpassing en tenuitvoerlegging van de gegevensbescherming zijn ook sanctiemogelijkheden tegen natuurlijke personen, en niet alleen tegen ondernemingen, voorzien. Dit betekent dat ook een toezichthouder voor gegevensbescherming of een bedrijfsleider persoonlijk aansprakelijk kan worden gesteld voor inbreuken en dat er eventueel een schadevergoeding kan worden verhaald op deze personen.

5. De countdown loopt: waar komt het op aan?

Ondanks mogelijke hoge geldstraffen en de snel aflopende overgangsperiode, hebben veel bedrijven nog geen voorzorgsmaatregelen getroffen. Volgens Gartner zal tegen einde 2018, wanneer de verordening allang in voege is getreden, altijd nog meer dan de helft van alle ondernemingen die onder de EU-AVG vallen, niet alle bepalingen hebben toegepast[2]. Met zo veel mogelijke gevolgen is het belangrijk een overzicht te verkrijgen van de zwaartepunten van de implementatie.

5.1. Toezichthouder voor gegevensbescherming aanduiden

De eerste stap is de aanduiding of aanstelling van een toezichthouder voor gegevensbescherming. Dit geldt conform artikel 37 voor overheidsinstanties, openbare ambten en ondernemingen, die persoonsgegevens verwerken. Voor kleine en middelgrote onderneming kan ook de benoeming van een externe toezichthouder voor gegevensbescherming worden overwogen. Deze moet zowel voor het publiek als tegenover de nationale gegevensbeschermingsautoriteit als officiële contactpersoon worden benoemd. Maar ook bedrijven die niet verplicht zijn een toezichthouder voor gegevensbescherming te benoemen, kunnen dit bijvoorbeeld benutten om een centraal punt voor interne en externe vragen betreffende gegevensbescherming op te zetten.

2 Bron: https://www.gartner.com/newsroom/id/3701117.

5.2. Brandpunten identificeren

Voor elke onderneming, ongeacht de grootte, kunnen de volgende vragen helpen de brandpunten voor de toepassing te identificeren:

- Welke van de gegevens die onderhevig zijn aan de EU-AVG worden in een onderneming verzameld en verwerkt?
- Worden de gegevens voldoende beschermd? Gebruikt de onderneming hulmiddelen conform de modernste beschikbare technologie ?
- Kan in het geval van een inbreuk op de gegevensbescherming binnen de 72 uur een melding naar de gegevensbeschermingsautoriteit worden gestuurd?
- Kunnen klanten informatie krijgen over de gegevens die over hen zijn opgeslagen of kunnen de gegevens worden verwijderd?
- Worden gegevens voor het opslaan of de verwerking ervan doorgegeven aan andere ondernemingen (bijv. clouddiensten)? Moeten hier eventueel aanpassingen aan de contracten worden uitgevoerd? Wat hier belangrijk is: er is geen “instandhoudingsbescherming” voor oude contracten.

5.3. Workflows en tools controleren

Hierbij moeten niet alleen de werknemers worden gesensibiliseerd voor het thema, maar moeten ook de workflows en tools worden gecontroleerd en eventueel naar een stand in overeenstemming met de wet worden gebracht. Het opstellen van richtlijnen over de omgang met informatie, is hier een belangrijke stap. Dergelijke regels vormen een combinatie van technische en organisatorische maatregelen. Zo kan policy management op technologieniveau ervoor zorgen dat alleen de tools die nodig zijn voor de gegevensverwerking, kunnen worden gebruikt, terwijl dat niet mogelijk is voor toepassingen zoals persoonlijke cloudopslagdiensten. Ook het gebruik van externe apparaten moet worden geblokkeerd zodat werknemers niet zomaar persoonsgegevens kunnen opslaan (bijvoorbeeld op USB-sticks).

5.4. De IT-infrastructuur controleren en beveiligen

Een andere belangrijke bouwsteen is de uitgebreide beveiliging van de IT-systemen. Bestaande systemen moeten worden gecontroleerd en nieuwe moeten eventueel worden ingepland en uitgerold. De bescherming begint al op netwerk- en communicatieniveau. Om niet toegelaten verbindingen te blokkeren, moet een firewall worden gebruikt. Webverkeer en andere communicatiepaden van internet moeten grondig worden gecontroleerd, bijv. door een webbeschermingscomponent of een e-mailscan. Bescherming tegen boosaardige malware kan met de hulp van een proactieve bewaking van het bestandssysteem en het proces worden gegarandeerd. Om ervoor te zorgen dat het besturingssysteem en de toepassingen up-to-date zijn en dat zwakke plekken tijdig worden opgelost, kan patch management erbij helpen het overzicht over de patchverdeling te behouden. Ook de gegevensbeveiliging is bijzonder belangrijk. Om te verhinderen dat de gegevens verloren gaan, moet een back-up- en herstelconcept worden uitgewerkt.

G DATA ondersteunt u bij het naleven van de EU-AVG

Om te kunnen voldoen aan de technische vereisten van de EU-AVG, moeten de beschermingscomponenten voor de IT-infrastructuur en processen optimaal op elkaar zijn afgestemd. Een uniform concept voor de bewaking van de netwerkinfrastructuur en de berichtgeving van de beheerder in het geval van een mogelijk incident met de gegevensbeveiliging, is cruciaal. Met de Layered Security-benadering biedt G DATA een totaaloplossing voor bedrijfsnetwerken van elke grootte, die een verfijnde proactieve bescherming combineert met efficiënte en accurate mogelijkheden voor een regelmatige rapportage en berichtgeving over voorvallen. U kunt de bedrijfsoplossingen van G DATA op uw eigen hardware installeren en deze zelf beheren. Indien gewenst kunt u ook met de hulp van de SaaS-oplossing G DATA Managed Endpoint Security de installatie- en beheerkosten uitbesteden. Fabrikantonafhankelijke diensten zoals penetratietests worden aangeboden door G DATA Advanced Analytics GmbH.

Meer informatie over de G DATA Business-oplossingen vindt u onder www.gdata.be/business. De G DATA Security Blog informeert u onder blog.gdata.de over de nieuwste ontwikkelingen op het vlak van gegevensbescherming, naleving en IT-veiligheid. Meer informatie over de diensten van G DATA Advanced Analytics GmbH vindt u onder www.gdata-advancedanalytics.de.

Houd ermee rekening dat deze whitepaper als inspiratiebron voor het omgaan met de mogelijke effecten van EU-AVG is uitgedacht en geen vervanging is voor uitgebreid juridisch advies.