UNIT4

Whitepaper

Unit4 en de Algemene Verordening Gegevens-bescherming (AVG) van de EU

In business for people.

Inhoud

Wat is de AVG?

Op 25 mei 2018 treedt een nieuwe Europese privacywet in werking: de Algemene Verordening Gegevensbescherming (AVG). Deze verordening is internationaal ook wel bekend onder de naam General Data Protection Regulation (GDPR).

Deze regelgeving zal in alle lokale privacywetten binnen de hele EU en Europese Economische Ruimte (EER) worden geïmplementeerd. De verordening geldt voor alle organisaties die producten of diensten verkopen aan burgers in Europa en hun persoonsgegevens verwerken, inclusief bedrijven op andere continenten. De verordening biedt burgers in de EU en EER meer controle over hun persoonsgegevens en moet waarborgen dat hun informatie in heel Europa goed wordt beschermd.

De nieuwe AVG vervangt de gegevensbeschermingsrichtlijn 95/46/EG. De AVG is rechtstreeks van toepassing in elke lidstaat en zal leiden tot een betere harmonisatie van gegevensbescherming tussen de EU-landen.

Hoewel veel bedrijven inmiddels al eigen privacyprocessen en -procedures hebben vastgesteld in overeenstemming met de richtlijn, bevat de AVG een aantal nieuwe waarborgen voor EU-Burgers waarvan gegevens worden verzameld. Zodra de AVG van kracht is, dreigen er forse boetes en straffen voor gegevensverantwoordelijken en verwerkers die zich niet aan de regels houden.

De AVG maakt het noodzakelijk dat bedrijven die persoonsgegevens van EU-Burgers verwerken hun verwerkingsproces zodanig aanpassen, dat deze in lijn is met de nieuwe Verordening.

Definities uit de AVG

In de AVG staat (de bescherming van) privacy centraal. Voor een goed begrip van de AVG is enige kennis van de 'AVG-terminologie' noodzakelijk. Onderstaand volgen de definities van enkele kernbegrippen.

Definities:

Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ('betrokkene'); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

Betrokkene: de natuurlijke persoon waarop de persoonsgegevens betrekking hebben.

Verwerkersverantwoordelijke: de natuurlijke persoon of rechtspersoon, overheidsinstantie, instelling of andere organisatie die - alleen of met anderen - de doeleinden en middelen van de verwerking van persoonsgegevens vaststelt. Soms worden de doeleinden en middelen voor de verwerking van persoonsgegevens echter bepaald door het recht van de Europese Unie of de specifieke lidstaat. In dat geval kan de gegevensverantwoordelijke (of kunnen de specifieke criteria voor het aanwijzen van een gegevensverantwoordelijke) ook worden geregeld in het recht van de Europese Unie of de specifieke lidstaat.

Verwerker: de natuurlijke persoon of rechtspersoon, overheidsinstantie, instelling of andere organisatie die persoonsgegevens verwerkt namens de verwerkingsverantwoordelijke.

Toestemming van de betrokkene: elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling de verwerking van zijn persoonsgegevens aanvaardt.

Gegevensinbreuk: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens.

Verwerking: een bewerking (of een geheel van bewerkingen) met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

Bereid uw organisatie voor op de nieuwe regelgeving

De Algemene Verordening Gegevensbescherming (AVG) stelt de nodige eisen aan het verzamelen, opslaan en gebruiken van persoonsgegevens, bijvoorbeeld met betrekking tot:

- Het identificeren en beveiligen van de persoonsgegevens in uw systemen
- Het voldoen aan de nieuwe transparantievereisten
- Het waarnemen en melden van gegevensinbreuken
- Het trainen van privacymedewerkers en andere werknemers.

We raden u aan om u voor te bereiden op de inwerkingtreding van de AVG door nu al aan de slag te gaan met 10 belangrijke stappen, zoals gedefinieerd door de Autoriteit Persoonsgegevens.

1. Bewustzijn
2. Rechten van betrokkenen
3. Overzicht van verwerking van persoonsgegevens
4. Data Protection Impact Assessment (DPIA)
5. 'Privacy by design' en 'privacy by default'
6. Functionaris voor de gegevensbescherming
7. Melding van gegevensinbreuken
8. Gegevensverwerkingsovereenkomsten
9. Leidende toezichthouder
10. Toestemming en wettelijk recht op verwerking van persoonsgegevens.

1. Bewustzijn

Zorg dat de relevante mensen in uw organisatie op de hoogte zijn van de nieuwe privacyregels. Zij moeten inschatten wat de impact van de AVG is op uw huidige processen, diensten en goederen en welke aanpassingen nodig zijn om aan de AVG te voldoen. Houd er rekening mee dat dit veel tijd en inzet van personeel kan vergen, dus begin hier op tijd mee.

2. Rechten van betrokkenen

Op grond van de AVG krijgen betrokkenen meer en uitgebreidere privacyrechten. U dient ervoor te zorgen dat zij hun privacyrechten naar behoren kunnen uitoefenen. Houd rekening met bestaande rechten, zoals het recht op inzage en het recht op correctie en verwijdering.
Maar vergeet ook nieuwe rechten niet, zoals het recht op gegevensoverdraagbaarheid. U moet ervoor zorgen dat de relevante gegevens beschikbaar zijn voor uw betrokkenen.

3. Overzicht van verwerking van persoonsgegevens

Registreer uw gegevensverwerking. Documenteer welke persoonsgegevens u verwerkt en voor welk doel. Documenteer waar deze informatie vandaan komt, waar deze is opgeslagen en met wie u deze deelt. Op grond van de AVG moet u kunnen aantonen dat uw organisatie voldoet aan de AVG.
Als de betrokkenen hun privacyrechten uitoefenen, hebt u mogelijk ook het overzicht nodig. Als zij u vragen hun persoonsgegevens te corrigeren of te verwijderen, moet u het verzoek ook doorgeven aan de organisatie(s) waarmee u deze gegevens hebt gedeeld.

4. Data Protection Impact Assessment (DPIA)

Bij een Data Protection Impact Assessment (DPIA) wordt de verwerking beschreven en worden de privacyrisico's beoordeeld en maatregelen vastgesteld. Een (D)PIA is alleen vereist als de verwerking "waarschijnlijk tot een hoog risico voor de rechten en vrijheden van natuurlijke personen zal leiden".

5. ‘Privacy by design’ en ‘Privacy by default’

- **Privacy by design** houdt in dat bescherming van persoonsgegevens onderdeel uitmaakt van het ontwerp van producten en diensten.
- **Privacy by default** betekent dat u technische en organisatorische maatregelen moet nemen om ervoor te zorgen dat de verwerking van persoonsgegevens standaard geoptimaliseerd wordt voor het specifieke doel en dat niet meer dan de minimaal benodigde persoonsgegevens worden verwerkt om het vooraf gedefinieerde doel te bereiken.

Unit4 R&D heeft deze principes vertaald naar “De 7 pilaren van ‘Privacy by design’ waarop de filosofie van Unit4 R&D is gebaseerd” (zie hier).

6. Functionaris voor de gegevensbescherming

Op grond van de AVG kunnen organisaties verplicht zijn om een functionaris voor de gegevensbescherming (FG) te benoemen. Ga na of dit ook voor uw organisatie geldt.

7. Melding van gegevensinbreuken

U dient alle gegevensinbreuken te documenteren. In geval van een gegevensinbreuk moet u deze goed gedocumenteerd melden aan de leidende toezichthouder. De leidende toezichthouder moet kunnen vaststellen of u hebt voldaan aan de rapportageplicht.

Unit4 heeft een intern protocol voor datalekken, dat u hier kunt nalezen. Als Unit4 de persoonsgegevens van uw organisatie bewaart, dan is het onvoldoende om enkel te vertrouwen op het interne protocol voor datalekken van Unit4. Uw eigen organisatie moet ook een protocol voor datalekken hebben.

8. Gegevensverwerkingsovereenkomst

Hebt u uw gegevensverwerking uitbesteed aan een verwerker? Ga dan na of de overeengekomen maatregelen in de bestaande contracten en gegevensverwerkingsovereenkomst met uw verwerker nog steeds afdoende zijn en voldoen aan de vereisten van de AVG. Is dat niet het geval, wijzig deze dan tijdig.

Unit4 heeft een standaard gegevensverwerkings-overeenkomst opgesteld die voldoet aan de huidige Richtlijn. Een nieuwe gegevensverwerkingsovereenkomst en aanvulling op de huidige gegevensverwerkings-overeenkomst zullen worden afgestemd op de AVG.

9. Leidende toezichthouder

Heeft uw organisatie vestigingen in meerdere EU-lidstaten? Of vindt uw gegevensverwerking in meerdere lidstaten plaats? Dan hebt u maar met één toezichthouder van doen. Dit wordt de leidende toezichthouder genoemd. Als dit voor uw organisatie geldt, ga dan na wie de leidende toezichthouder voor uw organisatie is.

Voor Unit4 is de Autoriteit Persoonsgegevens de leidende toezichthouder.

10. Toestemming en wettelijk recht op verwerking van persoonsgegevens

Uw gegevensverwerking kan gebaseerd zijn op de toestemming van de betrokkenen. De AVG stelt strengere eisen aan de toestemming voor de verwerking van persoonsgegevens. Evalueer en registreer daarom de manier waarop u toestemming vraagt. U moet kunnen aantonen dat de betrokkenen u toestemming hebben gegeven om hun persoonsgegevens te verwerken. En voor de betrokkenen moet het even gemakkelijk zijn om hun toestemming in te trekken als om deze te geven.

Binnen de AVG is het verzamelen en verwerken van persoonsgegevens slechts onder een van de volgende omstandigheden legitiem:

- als de betreffende persoon (de 'betrokkene'), na voldoende te zijn geïnformeerd, ondubbelzinnig toestemming heeft gegeven; of
- als de gegevensverwerking nodig is voor een contract, bijvoorbeeld voor facturering, een sollicitatie of een leningaanvraag; of
- als verwerking vereist is op grond van een wettelijke verplichting, of
- als verwerking noodzakelijk is om het vitale belang van de betrokkene te beschermen, bijvoorbeeld de verwerking van medische gegevens van een slachtoffer van een auto-ongeval; of
- als verwerking noodzakelijk is voor het vervullen van taken van algemeen belang of die door de overheid, de belastingdienst, de politie of andere overheidsorganen worden uitgevoerd; of
- Indien de gegevensverantwoordelijke of een derde daartoe een legitiem belang heeft, mits dit belang de belangen van de betrokkene niet schaadt of inbreuk maakt op zijn grondrechten, met name het recht op privacy. Deze bepaling schrijft voor dat er een redelijk evenwicht moet bestaan tussen de zakelijke belangen van de gegevensverantwoordelijke en de privacy van de betrokkene.

De AVG verbiedt de verwerking van persoonsgegevens waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging, het lidmaatschap van een vakbond en de verwerking van gegevens over de gezondheid of het seksleven, tenzij aan een van de uitzonderingscriteria is voldaan. Verwerkt uw organisatie dit soort persoonsgegevens? Dan is het raadzaam om u te verdiepen in de uitzonderingscriteria.

Bijlage 1: **Unit4 en de AVG**

Privacy (en daarmee de AVG) geniet de hoogste prioriteit bij Unit4. Unit4 bereidt zijn mensen, producten en processen voor om te voldoen aan de vereisten van de Algemene Verordening Gegevensbescherming van de EU ('AVG'), die op 25 mei 2018 van kracht wordt. Uiteraard zal Unit4 voldoen aan de verplichtingen binnen de AVG, alsook aan de verplichtingen die op grond van nationale wetgeving kunnen worden opgelegd.

Hieronder worden de belangrijkste elementen uit de AVG en de acties die Unit4 onderneemt toegelicht.

'Privacy by design'

Als onderdeel van de R&D-processen voor de verschillende producten van Unit4 wordt een audit uitgevoerd, samen met een externe auditor, om vast te stellen welke stappen moeten worden ondernomen om het 'Privacy by design'-concept te implementeren in de ontwikkelingscyclus.

De aanbevelingen van de audit worden als uitgangspunt genomen voor de ontwikkeling van nieuwe producten die na 25 mei 2018 op de markt komen. In dit proces wordt het 'Privacy by default'-concept eveneens overwogen. Voor andere functies, zoals support, professionele service en cloudservices, vindt een evaluatie plaats om vast te stellen in welke impact het 'Privacy by design'-concept heeft en welke maatregelen moeten worden genomen.
Een overzicht van 'Privacy by design' bij Unit4 R&D vindt u in bijlage 3.

Verwerkersovereenkomsten

Op dit moment verwerkt Unit4 al persoonsgegevens namens zijn klanten. Deze verwerking vindt – in de meeste gevallen – plaats op basis van een bewerkingsovereenkomst. Deze overeenkomsten zullen worden geëvalueerd en afgestemd op de nieuwe vereisten op grond van de AVG, zoals (zonder beperkingen) de geheimhoudingsplicht voor werknemers, een beschrijving van technische en organisatorische maatregelen op het gebied van gegevensbeveiliging, en de verantwoordelijkheids- en auditvereisten. De bewerkersovereenkomst heet onder de AVG een verwerkersovereenkomst

Registratie van verwerking

Unit4 zal alle verwerkingsactiviteiten registreren en documenteren conform de vereisten van de AVG. De opzet en structuur van het register worden bepaald door de interne IT-afdeling en R&D-afdeling van Unit4.
Gegevensbeveiligingsvoorschriften
De gegevensbeveiligingsvoorschriften binnen de AVG zijn min of meer hetzelfde als de richtlijnen van de Autoriteit Persoonsgegevens, waaraan Unit4 voldoet.

Datalekken

De verplichtingen voor Unit4 om datalekken binnen een tijdsbestek van 72 uur (zoals bepaald in de AVG) te melden aan de verantwoordelijke autoriteit zullen worden nagekomen. Unit4 heeft een intern protocol voor datalekken, dat zal worden bijgewerkt in lijn met de AVG.

Privacy-effectbeoordeling

Unit4 zal een privacy-effectbeoordeling, onder de AVG ook wel een Data Protection Impact Assessment (DPIA) of Privacy Impact Assessment (PIA) genoemd, uitvoeren als er een hoog risico bestaat voor de verwerking van persoonsgegevens en zal de privacy-effectbeoordeling indien nodig tot een integraal onderdeel van zijn processen maken.

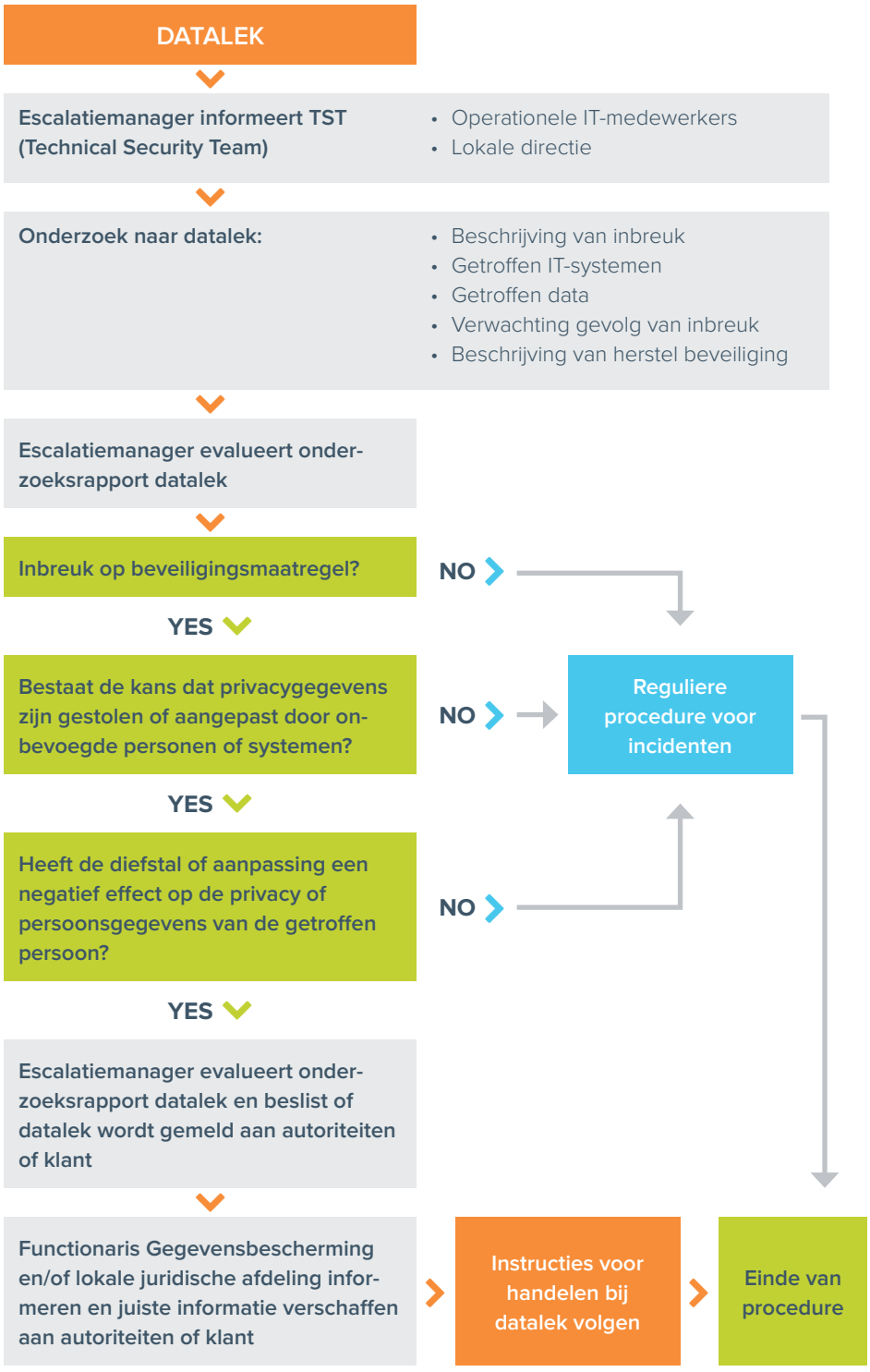
Functionaris voor de gegevensbescherming

Gegevensbescherming is onderdeel van de Global Information Security-functie binnen Unit4. Als zodanig is deze functie verantwoordelijk als functionaris voor de gegevensbescherming in het kader van de AVG. In bepaalde landen waarin Unit4 actief is, zullen desgewenst lokale functionarissen voor de gegevensbescherming worden benoemd om de naleving op lokaal niveau te garanderen.

Audits en accreditaties

Unit4 evalueert, welke audits en accreditaties vereist zijn voor de diensten die bedrijf levert en mogelijk moeten worden aangepast conform de AVG. De accreditatie kan verschillen per product, dienst of land waar het product of de dienst wordt aangeboden aan het publiek.

Bijlage 2: **Protocol van Unit4 voor datalekken**



Bijlage 3: **‘Privacy by design’ vanuit Unit4 R&D**

De Algemene Verordening Gegevensbescherming (AVG) is een geharmoniseerde aanpak om in heel Europa aan de wetgeving inzake privacybescherming te voldoen. De AVG beschouwt ‘Privacy by design’ als een wettelijke verplichting voor gegevensverantwoordelijken en verwerkers en verplicht ‘Privacy by default’.

Privacy by design richt zich op het inbedden van privacybeschermingsmaatregelen in producten en het hele ontwikkelingsproces van producten, processen of diensten die gebruik kunnen maken van persoonsgegevens. ‘**Privacy by design’** werd lang gezien als een ‘best practice’, maar zal op grond van de AVG verplicht zijn.

De aanpak van Unit4 R&D

Unit4 R&D gelooft dat de doelen het best worden gehaald als onderdeel van een totaalaanpak om privacy te beschermen. Een van de acties om dat te bereiken is de beoordeling die jaarlijks wordt uitgevoerd om het productrisico te identificeren/verifiëren, rekening houdend met verschillende aspecten. Een van de categorieën die wordt gebruikt om de productrisicoindex te definiëren, heeft betrekking op de vereiste niveaus van vertrouwelijkheid en integriteit voor de gegevens die door de applicatie worden opgeslagen.

Unit4 R&D erkent het belang van ‘Privacy by design’ en ‘Privacy by default’ om privacyrisico’s te minimaliseren en vertrouwen op te bouwen. Unit4 R&D houdt zich aan eerdere privacyregelgeving en werkt aan de integratie van ‘Privacy by design’-basisprincipes als onderdeel van de softwareontwikkelings-levenscyclus. We streven ernaar om onze geïntegreerde principes uit te breiden en te versterken.

De 7 pilaren van ‘Privacy by design’ waarop de filosofie van Unit4 R&D is gebaseerd

1e pijler – Proactief en preventief

Onze aanpak stelt mensen, processen en technologieën voorop om privacybescherming te implementeren en te verbeteren. Om privacy in onze producten te integreren, streeft Unit4 R&D ernaar om zijn personeel optimale scholing te bieden. Gegevensbescherming, ‘Privacy by design’ en applicatiebeveiliging zijn onderdeel van het opleidingsprogramma.

2e pijler – Privacy by default

‘Privacy by default’ verwijst naar het implementeren van mechanismen om ervoor te zorgen dat persoonsgegevens ‘standaard’ alleen voor de opgegeven doeleinden worden verwerkt. Het is een ontwerpconcept dat ruim is gedefinieerd om het verzamelen, weergeven of delen van persoonsgegevens zonder uitdrukkelijke toestemming van de betrokkene te verbieden. In een meer gedetailleerde weergave beslaat dit standaard de meest restrictieve privacyinstellingen. Met andere woorden: zelfs wanneer de gebruiker niets doet, is zijn privacy beschermd.
Dit concept is onderdeel van onze standaardvereisten voor nieuwe functies en producten. Ons beleid is erop gericht om méér controle over privacy te bieden, in plaats van minder. Klanten hebben de mogelijkheid om Unit4 producten zodanig te configureren dat ze voldoen aan hun eigen interne vereisten.

Unit4 R&D gaat na of ons privacy- en cookiebeleid voldoet aan de vereisten die de AVG stelt.

3e pijler – Geïntegreerd in het ontwerp

De ontwikkelrichtlijnen en -procedures voor ‘Privacy by design’ zijn beschikbaar in onze interne technische kennisdatabase, die is gewijd aan alle Unit4 producten.

Unit4 R&D werkt vanaf het allereerste begin aan het integreren van privacy in het ontwerp, de architectuur en functionaliteit.
Privacy wordt hierdoor een geïntegreerd onderdeel van het systeem, zonder dat dit ten koste gaat van de functionaliteit.

4e pijler – Volledige functionaliteit

Bij Unit4 R&D wordt alles in het werk gesteld om ervoor te zorgen dat privacy, veiligheid en functionaliteit in onze producten worden geïmplementeerd. We zijn bezig om de cultuur van het ‘positieve som’-concept te implementeren, wat inhoudt dat er geen overheersend concept is. Privacy verdient niet alleen in een vroeg stadium, maar gedurende de gehele softwareontwikkelingslevenscyclus aandacht.

5e pijler – Complete beveiliging

In onze aanpak is beveiliging een essentieel aspect om privacy te garanderen. Unit4 R&D heeft richtlijnen opgesteld voor het implementeren van beveiliging als onderdeel van de softwareontwikkelingslevenscyclus, op basis van beveiligingsframeworks van OWASP. We zijn bezig om de standaard volledig te implementeren en onze medewerkers te trainen.

Unit4 heeft een Security Community met vertegenwoordigers voor elk product en andere gerelateerde gebieden. We hebben een Global Penetration Testing-programma, waarbij voor elke belangrijke release van relevante producten – door een externe en onafhankelijke partij beveiligingstests worden uitgevoerd, gebaseerd op risico en levenscyclus. Het doel hiervan is om zwakke plekken in de beveiliging bloot te leggen en actief te misbruiken om kwetsbaarheden aan te tonen.

6e pijler – Inzichtelijkheid en transparantie

Unit4 R&D biedt onze klanten inzichtelijkheid en transparantie door externe partijen audits en certificeringen te laten uitvoeren en beschikbaar te stellen.
We bieden onze klanten volledige transparantie en inzichtelijkheid door documentatie van de geïntroduceerde functionaliteit te creëren. Als er voor de verwerking van privégegevens gebruik wordt gemaakt van onderdelen van derden, zullen deze specifiek worden vermeld in een gegevensverwerkingsovereenkomst.

7e pijler – Respect voor privacy van de gebruiker

‘Privacy by design’ en ‘Privacy by default’ zijn kernwaarden voor softwareontwikkeling door Unit4 R&D. Wij geloven dat door de gebruiker centraal te stellen, alle andere principes ook op hun plaats vallen. We willen onze klanten helpen om tegemoet te komen aan hun eigen AVG-nalevingsvereisten door in hoge mate configureerbare functionaliteit te bieden.

Over Unit4

Unit4 is een toonaangevende leverancier van gebruiksvriendelijke bedrijfssoftware voor dienstverlenende organisaties. Met een jaaromzet van bijna 600 miljoen euro en meer dan 4200 werknemers over de hele wereld levert Unit4 hoogwaardige ERP- en bedrijfssoftware voor diverse branches. Duizenden organisaties uit diverse sectoren, waaronder professionele dienstverlening, publieke dienstverlening, non-profit, onroerend goed, groothandel, financiële dienstverlening en onderwijs, profiteren van de oplossingen van Unit4.

unit4.nl

Unit4 Business Software B.V.
Papendorpseweg 100, 3528 BJ Utrecht
Postbus 5005, 3502 JA Utrecht
T +31 88 247 17 77
E info.group@unit4.com