December 2019

Beleid voor Gegevensbescherming

Informatiebeveiliging & Privacy

UNIT4
BEDRIJFSSOFTWARE

Inhoudsopgave

Document eigenschappen

Auteur	:	Roald Roos
Goedgekeurd door	:	Information Security Risk Board
Versie	:	1.2
Datum	:	December 2019
Classificatie	:	Publiek

Introductie

Deze standaard beschrijft de aanpak van Unit4 Bedrijfssoftware om informatiebeveiliging en privacyrisico's met betrekking tot het verzamelen, opslaan, verwerken en verwijderen van alle gegevens van klanten ("Klantgegevens") ongeacht of deze klanten al voormalige klanten zijn, of prospects en/of individuen, eenmanszaken, partners of bedrijven ('Klanten'). Dit document maakt deel uit van het 'Unit4 Bedrijfssoftware Security Framework' en biedt gedetailleerde vereisten om te voldoen aan de informatiebeveiligingsdoelstellingen van de door Unit4 Bedrijfssoftware geadopteerde 'Global Information Security Policy'.

Dit beleid is ontworpen

- om het risico voor Unit4 Bedrijfssoftware bij het verwerken en verwerken van klantgegevens te verminderen (d.w.z. het risico dat gegevens verloren gaan, inclusief als gevolg van diefstal);
- om controleerbare en aantoonbare controles op de verwerking van klantgegevens in te stellen;
- om te zorgen voor naleving van wettelijke principes, waaronder dat klantgegevens:
    - niet langer bewaard worden dan nodig wordt geacht om het doel te bereiken waarvoor het werd verzameld; en
    - niet verwerkt wordt voor enig ander doel (en) dan waarvoor het is verzameld.

Voor wie geldt dit beleid?

Dit beleid is van toepassing op alle Unit4 Bedrijfssoftware -medewerkers en ingehuurde partijen die namens of in opdracht van Unit4 Bedrijfssoftware werkzaamheden verrichten.

Heb je vragen of opmerkingen over dit beleid, neem dan contact op met afdeling Informatiebeveiliging en Privacy.

Versiebeheer

Versie	Datum	Auteur	Samenvatting van wijzigingen
1.0	Maart 2019	Kenny den Hollander	Eerste opzet
1.1	28-03-2019	Kenny den Hollander	Kleine aanpassingen
1.2	5-12-2019	Roald Roos	Vertaling NL, Huisstijl Unit4 Bedrijfssoftware

Beleidsregels

Wanneer worden klantgegevens verzameld?

Wanneer er gemigreerd, opgeslagen of verwerkt wordt binnen een Software as a Service (‘Saas’) of Cloud-omgeving, beheerd door Unit4 Bedrijfssoftware. Het data-eigendom van deze klantgegevens wordt NIET overgedragen aan Unit4 Bedrijfssoftware. De klant blijft ‘datacontroller’ terwijl Unit4 Bedrijfssoftware functioneert als ‘dataprocessor’. Aanvullende verwerkersovereenkomsten bepalen de gedetailleerde rol van Unit4 bij het verwerken en beschermen van deze klantgegevens.

Het is het beleid van Unit4 Bedrijfssoftware dat het verzamelen van klantgegevens, met name ‘live data’, een ‘laatste redmiddel’ moet zijn. Unit4 Bedrijfssoftware moet ernaar streven alleen klantgegevens te verzamelen en te verwerken wanneer dit van vitaal belang is voor het oplossen van een support- of technisch probleem, het uitvoeren van een overeenkomst met de klant of vereist is voor productontwikkeling, verificatie en/of validatie.

Het is het beleid van Unit4 Bedrijfssoftware dat het verzamelen van 'gevoelige’ persoonsgegevens (gegevens die betrekking hebben op iemands raciale of etnische afkomst, politieke opvattingen, religieuze overtuigingen of andere soortgelijke opvattingen, vakbondslidmaatschap, lichamelijke of geestelijke gezondheidstoestand, seksuele geaardheid, het hebben gepleegd of vermeende plegen van een misdrijf of procedure voor een feitelijk of vermeend misdrijf, de beschikking over een dergelijke procedure of de veroordeling van een rechtbank in een dergelijke procedure) moet worden vermeden. Als het verzamelen van dit soort persoonlijke gegevens onvermijdelijk is, moeten de gegevens duidelijk worden gemarkeerd als ‘Gevoelig’ en aan aanvullende beveiligingsmaatregelen worden onderworpen.

Hoe moeten klantgegevens worden verzameld?

Als het nodig is om klantgegevens te verzamelen op basis van een of meer van de in vorige paragraaf genoemde redenen, moeten de klantgegevens rechtstreeks van de klant worden verzameld en niet van een derde partij (tenzij u de toestemming van de klant hebt). Om aan deze eis te voldoen, moeten de volgende punten worden overwogen:

Waar mogelijk dient de klant verzocht te worden ‘testgegevens’ (d.w.z. niet ‘live gegevens’) in te dienen. Het type gegevens dat wordt verstrekt, moet altijd duidelijk worden aangegeven als ‘testgegevens’ of ‘live gegevens’. Er moet een e-mail of een alternatieve vorm van schriftelijke bevestiging van de klant ontvangen zijn dat de klantgegevens ‘testgegevens’ zijn. Als er geen schriftelijke bevestiging is, moet ervan uitgegaan worden dat klantgegevens ‘live data’ zijn. Waar praktisch mogelijk dienen er nooit gegevens te worden geaccepteerd met live persoonlijke bankrekeningen of creditcardgegevens, en moet - waar praktisch mogelijk - de klanten gevraagd worden om dergelijke gegevens door elkaar te gooien of te verwijderen voordat deze aan Unit4 Bedrijfssoftware verstrekt worden.

Klanten moeten altijd worden geïnformeerd over:

- **De doelstelling (en)** waarvoor Unit4 Bedrijfssoftware hun gegevens verzamelt en verwerkt;
- De **identiteit van Unit4** Bedrijfssoftware als ‘gegevensverwerker’ voor wettelijke doeleinden en hoe zij contact kunnen opnemen met Unit4 Bedrijfssoftware;
- Hoe hun gegevens worden **opgeslagen** door Unit4 Bedrijfssoftware;
- Hun rechten met betrekking tot het verzamelen en verwerken van hun gegevens, inclusief maar niet beperkt tot, het **recht op toegang**, het **recht op rectificatie**, het **recht om te wissen**, het **recht op gegevensoverdraagbaarheid** en het **recht om bezwaar te maken**.

Wanneer klantgegevens elektronisch worden verstrekt, moet het doel zijn ervoor te zorgen dat passende beveiligingsmaatregelen zijn getroffen om de klantgegevens te beschermen wanneer deze worden overgedragen van de klant naar Unit4 Bedrijfssoftware. Dergelijke beveiligingsmaatregelen omvatten, maar zijn niet beperkt tot:

- **Veilige ftp-methoden** (file transfer protocol). Supportdesk en technische afdelingen beschikken over passende middelen om dit te bieden wanneer dat nodig is;
- **Verwijderbare media (bijv. CD/DVD/harde schijf/tapemedia)** verzonden per beveiligde of geregistreerde post; en
- **Versleutelde e-mail** wanneer andere methoden niet beschikbaar zijn, of voor urgentie namens de klant.

Voordat 'live data' wordt geaccepteerd, moet toestemming gevraagd worden aan lokale kwaliteitsmanager (waar van toepassing), leidinggevende of de DPO.

Er moet altijd overwogen worden of klantgegevens moeten worden overgedragen aan andere bedrijven binnen de Unit4 -groep of andere derde partijen (bijvoorbeeld om een serviceaanvraag te verstrekken). Als klantgegevens moeten worden overgedragen aan een andere partij, moet de klant altijd op de hoogte worden gebracht en moet zijn toestemming worden verkregen voordat de overdracht plaatsvindt. Gevoelige gegevens (zoals beschreven in voorgaande paragraaf) mogen nooit worden overgedragen buiten de Europese Economische Ruimte (EER). Voor elke wijziging in het gegevensoverdrachtsproces moet toestemming van de klant worden verkregen.

Het is belangrijk om te onthouden dat zodra Klantgegevens zijn verzameld, deze alleen door Unit4 Bedrijfssoftware mogen worden bewaard zolang er een zakelijke noodzaak is om deze te bewaren of zoals vereist onder toepasselijke bewaartermijnen voor gegevens. Voor elk gegevensverwerkingsproces moet een bewaarschema zijn opgesteld om ervoor te zorgen dat gegevens worden bewaard in overeenstemming met de AVG en andere toepasselijke wetgeving. Bij vragen over deze bewaartermijnen, neem dan contact op met uw lokale kwaliteitsmanager (waar van toepassing) of Data Protection Officer.

Beperkingen op het gebruik van klantgegevens

Het gebruik van klantgegevens is gebonden aan beperkingen. Klantgegevens moeten:

- Alleen toegankelijk en gebruikt worden als er een specifiek zakelijk doel voor is;
- Niet worden:
  - Gebruikt voor elektronische direct marketing (bijvoorbeeld per e-mail, fax, telefoon en/of sms) zonder vooraf de toestemming van de klant voor dergelijk gebruik te hebben verkregen;
  - Gebruikt voor uw eigen persoonlijke doeleinden; of
  - Gedeeld met derden (tenzij goedgekeurd door de klant)

Wanneer er een zakelijke behoefte is om toegang te krijgen tot en klantgegevens te gebruiken, moet:

- Klantgegevens alleen gebruikt worden voor het doel waarvoor deze zijn verzameld; en
- Toestemming gevraagd worden als de klantgegevens voor een nieuw doel gebruiken moeten worden.

Bewaring van klantgegevens

Alle klantgegevens moeten onmiddellijk na voltooiing van het doel waarvoor ze zijn verzameld, worden verwijderd of aan de klant worden geretourneerd, tenzij Unit4 Bedrijfssoftware:

- Nadrukkelijk gevraagd is om het te bewaren door de klant; of
- Vereist is om de klantgegevens te bewaren in overeenstemming met toepasselijke bewaartermijnen voor gegevens. Bij vragen over deze bewaartermijnen, neem contact op met de supportafdeling of de Data Protection Officer.

Klantgegevens die worden bewaard door Unit4 Bedrijfssoftware mogen alleen worden opgeslagen in afgesloten ruimtes (bij voorkeur in kluisjes) en mogen niet - waar praktisch mogelijk - worden opgeslagen op Unit4 Bedrijfssoftware - laptops of andere mobiele opslagmedia.

Verzoeken van klanten met betrekking tot klantgegevens

Wanneer een klant zijn/haar rechten uitoefent met betrekking tot het verzamelen en verwerken van zijn gegevens, **moet** een dergelijk verzoek onmiddellijk geëscaleerd worden naar supportmanager, of de Data Protection Officer.

Algemene opmerkingen over klantgegevens buiten het kantoor

Het is het beleid van Unit4 Bedrijfssoftware dat klantgegevens (of dat nu 'live data' of 'testdata' zijn) **niet off-site** op laptops, geheugensticks, USB-sticks, CD of andere opslagmedia mogen worden opgeslagen **zonder schriftelijke toestemming** van zowel de klant **en** verantwoordelijk manager.

Wanneer toestemming is verkregen, **zorgt verantwoordelijke medewerker** ervoor dat:

- De klantgegevens en opslagmedia waarop deze worden bewaard, niet worden achtergelaten in een ontgrendelde auto of onbeheerd op een plaats waar ze door anderen kunnen worden bekeken of verwijderd; en
- Alle beveiligingssystemen op de opslagmedia waarop de klantgegevens worden bewaard (zoals wachtwoordbeveiliging en schijfversleuteling) worden geactiveerd.

unit4bedrijfssoftware.nl

Unit4 Bedrijfssoftware
Papendorpseweg 100
3528 BJ Utrecht