Würth Belux
Privacy Management Systeem

Privacybeleid

Document type:	Beleid
Omgeving:	Privacy Management Systeem
Versie:	V1
Creation date:	12/07/2018
Document eigenaar:	
Classificatie	Intern gebruik
Laatste modificatie:	5/10/2018
Laatste review:	Click here to enter a date.
Goedkeuring management:	Click here to enter a date.
Opmerkingen:	[Comments]

Document Informatie

Confidentialiteitsclausule

Alle informatie die in dit document wordt gepubliceerd, is geclassificeerd als uitsluitend voor intern gebruik en zal daarom alleen worden vrijgegeven aan werknemers van Würth Belux (hierna Würth). Leveranciers, contractanten... krijgen toegang tot dit document na ondertekening van een geheimhoudingsovereenkomst om de naleving van het Würth privacy- en informatieveiligheidsbeleid, -normen en -procedures te verzekeren.

Verklaring van overeenstemming

Alle privacy- en informatiebeveiligingsdocumentatie is afgestemd op de juridisch bindende elementen van het arbeidscontract van Würth. Wettelijke en contractuele vereisten worden geïmplementeerd waar van toepassing.
Over het algemeen is de Würth-documentatie inzake informatiebeveiliging en privacy een verfijning en een verdere uitbreiding van de wettelijke en contractuele bindende bepalingen die van toepassing zijn op iedereen die toegang heeft tot informatie van Würth en deze informatie gebruikt, creëert of verwerkt.

1 Introductie

1.1 Doelstelling

Würth is zich ervan bewust dat haar werking steunt op persoonsgegevens en dat we de privacy dienen te respecteren en beschermen van alle natuurlijke personen, met inbegrip van klanten, bezoekers van de website, medewerkers, leveranciers en eventuele andere betrokkenen. Gepaste maatregelen moeten genomen worden om er zeker van te zijn dat wij conform de AVG-wetgeving zijn en persoonsgegevens beschermd zijn tegen ongeoorloofd gebruik, bekendmaking wijziging of vernietiging, zowel opzettelijk als onopzettelijk.
De Data Protection Officer (DPO) volgt de naleving van dit beleid op.

1.2 Toepasbaarheid

Dit privacybeleid is van toepassing voor het volledige management, alle medewerkers van Würth (inclusief tijdelijke werknemers) en elke contractant die namens Würth (consultants en andere derde partijen) persoonsgegevens verwerkt.

1.3 Reikwijdte

Dit privacybeleid is van toepassing op alle bedrijfsactiviteiten die uitgevoerd worden door Würth waarbij persoonsgegevens in elke mogelijke vorm verwerkt worden.

1.4 Referenties

Dit privacybeleid refereert naar de nieuwe AVG-wetgeving 2016/679 (AVG/GDPR) van het Europees Parlement en de Europese Raad en de informatieveiligheidsstandaard ISO27001:2013.

1.5 Definities

Betrokkene	De natuurlijke persoon waarvan persoonsgegevens worden verwerkt. Dit kunnen klanten, bezoekers van de website, medewerkers, leveranciers... zijn.
Persoonsgegevens	Alle gegevens die verband houden met een geïdentificeerde of (indirect) identificeerbare natuurlijke persoon via eender welk medium met inbegrip van e-mail, papier, instant messaging, databases, websites, videobeelden, geluidsopnames...
Gevoelige persoonsgegevens	Bepaalde categorieën persoonsgegevens die een hoger beschermingsniveau vereisen, met name persoonsgegevens in verband met ras of etnische afkomst, religieuze of levensbeschouwelijke opvattingen, lidmaatschap bij een vakbond, politieke standpunten, gezondheid en vermeende of gepleegde strafbare feiten.
Verwerkingen	Activiteiten die verzameling, gebruik, opslag, verandering, verzending, overdracht, verspreiding, bekendmaking of verwijdering van persoonsgegevens omvatten, en behoren tot het toepassingsgebied van dit beleid.

2 Privacybeleid

Betrokkenen verwachten van Würth dat ze hun persoonsgegevens verzamelen en gebruiken op een rechtmatige manier, conform met de AVG-wetgeving. De volgende essentiële principes vormen een basis om ervoor te zorgen dat Würth deze verwachtingen inlost en voldoet aan de AVG-wetgeving:

1. Het **verzamelen en gebruik van persoonsgegevens** moet op een eerlijke en wettelijke manier gebeuren en enkel voor rechtmatige doeleinden;

2. Het verzamelen van persoonsgegevens gebeurt steeds met de nodige **informatie voor en communicatie naar de betrokkene** m.b.t. de verwerking van zijn/haar persoonsgegevens;

3. **Het beheer van persoonsgegevens** moet conform zijn met de vooropgestelde kwaliteitsnormen en bewaartermijnen;

4. De **rechten van de betrokkenen** met betrekking tot hun persoonsgegevens moeten gerespecteerd worden;

5. (Vermoedelijke of effectieve) **gegevenslekken** van persoonsgegevens moeten gemeld en onderzocht worden;

6. Het **bewustzijn van medewerkers en andere contractanten** moet aanwezig zijn en continu verbeterd worden m.b.t. het verwerken van persoonsgegevens;

7. Er moeten gepaste **technische en organisatorische veiligheidsmaatregelen** geïmplementeerd worden om persoonsgegevens te beschermen.

2.1 Verzamelen en gebruik van persoonsgegevens

Het eerlijk en wettelijk **verzamelen en gebruik van persoonsgegevens** moet gewaarborgd worden door:

- Het beperken van het verzamelen van persoonsgegevens tot wat vereist en toegelaten is zoals voorzien in SAP, Speedy Touch, gegevensdragers en andere standaard templates, gecontroleerd door de DPO. Het verzamelen van vele andere persoonsgegevens (bv. informatie over familieleden van klanten) is niet toegelaten;

- Het respecteren van de keuze indien prospecten, klanten... geen interesse meer hebben in verder contact, inclusief het contacteren van klanten door ondermeer Telesales.

- Het respecteren indien een klant zijn toestemming intrekt voor e-mailmarketing.

Opmerking: Accountmanagers moeten in de nabije toekomst gebruik maken van een maillijst zodat deze voorkeuren gerespecteerd worden. Hierover zal nog gecommuniceerd worden.

- Het enkel voor rechtmatige doeleinden verzamelen van persoonsgegevens of wanneer het bij wet vereist is. De verzamelde persoonsgegevens mogen niet gebruikt worden voor andere niet-verenigbare doeleinden dan waarvoor ze verzameld zijn, of hier moet toestemming voor gevraagd worden;

- Het verbieden van het meedelen van persoonsgegevens aan externen, dit mag enkel indien dit bij wet verplicht is (bv. juridische instanties) of noodzakelijk is voor de gepaste en rechtmatige doeleinden en met de nodige garanties (NDA, verwerkersovereenkomst). Voorafgaand moet hiervoor eerst de DPO geconsulteerd worden;

- Het verbieden van het transfereren van persoonsgegevens buiten de Europese Economische Ruimte (EER) zonder een voorafgaande analyse en goedkeuring van de DPO.

2.2 Informatie voor en communicatie naar de betrokkene

De nodige **informatie voor en communicatie naar de betrokkene** m.b.t. de verwerking van zijn/haar persoonsgegevens moet gewaarborgd worden door:

- Het documenteren en publiceren van de nodige privacyverklaringen die specifiek zijn opgesteld voor de verschillende betrokkenen (klanten en (potentiële) werknemers);

- Het eenvoudig beschikbaar maken van de privacyverklaringen, namelijk op de website voor klanten en op het intranet voor werknemers;

- Het actief communiceren van de privacyverklaring d.m.v. een automatische bevestigingsmail bij registratie in SAP met een verwijzing naar de privacyverklaring;

- Het actief communiceren van de privacyverklaring bij indiensttreding van nieuwe werknemers;

- Het mondeling verwijzen naar de privacyverklaring op de website bij vragen over zijn of haar privacy;

- Het meedelen van de bron bij eerste communicatie indien persoonsgegevens zijn verkregen via andere bronnen dan de betrokkene (bv. Trendstop, KBO, LinkedIn).

- Het up-to-date houden van de privacyverklaringen a.d.h.v. periodieke reviews en ad-hoc wijzigingen bij nieuwe verwerkingen.

2.3 Beheer van persoonsgegevens

Het conform intern **beheren van persoonsgegevens** moet gewaarborgd worden door:

- Persoonsgegevens moeten nauwkeurig en juist zijn, en indien nodig geactualiseerd indien er voor een tijd van ongeveer 2 jaar geen contact meer is geweest. Dit kan via onze website en hiervoor rekenen we op onze werknemers die de persoonsgegevens gaan controleren bij een eerstvolgend contact;

- Persoonsgegevens mogen niet langer bewaard worden dan nodig is voor de doeleinden waarvoor ze worden verzameld. Dit komt voor prospecten neer op een termijn van maximaal 3 jaar en klanten maximaal tot 10 jaar na de laatste aankoop. Voor werknemers komt dit neer op een maximale termijn van 5 jaar na uitdiensttreding. Na deze termijnen worden al deze persoonsgegevens (automatisch) verwijderd.

2.4 Rechten van de betrokkenen

De **rechten van de betrokkenen** met betrekking tot hun persoonsgegevens moeten gerespecteerd worden. Indien een klant een recht wenst uit te oefenen moet er worden doorverwezen naar de privacyverklaring op de website zodat de klant bij de juiste mensen terechtkomt, op uitzondering van het recht op aanpassing van zijn of haar persoonsgegevens. Dit recht mag wel door een werknemer worden uitgevoerd.

De rechten van betrokkenen omvatten:

- Het recht op toegang tot de persoonsgegevens die over hem/haar bijgehouden worden,
- Het recht op aanpassing van onjuiste of onvolledige persoonsgegevens;
- Het recht op gegevenswissing of vergetelheid;
- Het recht op stopzetting van de verwerking van zijn/haar persoonsgegevens;
- Het recht om zijn persoonsgegevens naar een andere verantwoordelijke over te brengen;
- het recht om bezwaar aan te tekenen tegen direct marketing en elk gebruik van persoonsgegevens dat (mogelijks) nadelige gevolgen heeft voor de betrokkene;
- Het recht om een klacht in te dienen indien zijn of haar privacy niet wordt gerespecteerd.

Würth organiseert zich hierop via de mailbox privacy@würth.be, vermeld in de privacyverklaring op de website.

2.5 Melding van gevenslekken

- Wat is een gegevenslek en informatieveiligheidsincident
  - Een gegevenslek is een situatie waarin persoonsgegevens minstens dreigen ongeoorloofd te worden openbaar gemaakt, verloren te gaan, vernietigd of gewijzigd te worden. Een vermoeden volstaat dus.
    - Voorbeelden
      - Verlies van papieren dossiers met persoonsgegevens
      - Ongeoorloofde inzage in papieren en online dossiers met persoonsgegevens
      - Verlies van een niet-sterk geëncrypteerde usb-stick (met persoonsgegevens), laptop, gsm...
      - Verkeerde externe afzender van een e-mail met in bijlage een lijst van persoonsgegevens
      - Het delen van persoonsgegevens op het internet
      - Gehackte computer, Ipad,...
  - Een informatieveiligheidsincident heeft betrekking op niet-persoonsgegevens (bijvoorbeeld strategisch belangrijke of financiële documenten). Dergelijke incidenten kunnen aanleiding geven tot reputatieschade, verlies van vertrouwen, rechtszaken en het niet voldoen aan wettelijke vereisten.

- Waar moet ik dit melden
  - U moet dit zo snel als mogelijk melden aan de helpdesk via de volgende contactgegevens:
    - helpdesk@wurth.be

  - Indien u van oordeel bent dat het een kritisch gegevenslek of incident is dat de reputatie en de continuïteit van Würth Belux mogelijk in het gedrang kan brengen, verzoeken wij u om de helpdesk zo snel als mogelijk te telefoneren op het volgende nummer:
    - 014/44.55.12

  - Bij het verlies van een laptop of Ipad moet u ook steeds de politie verwittigen.

- Wat moet ik melden
  - Indien u een gegevenslek of incident ontdekt, moet u dit onmiddellijk melden met de volgende informatie:
    - Uw eigen contactgegevens;
    - Vermelding dat het om een gegevenslek of incident gaat of u dit toch vermoedt;
    - Korte beschrijving van het (vermoedelijke) gegevenslek of incident:
      1. Soort gegevenslek of incident;
      2. Inschatting van het aantal personen waarvan gegevens zijn gelekt (bij gegevenslek);

3. Van wie zijn de gegevens, bijvoorbeeld werknemers, klanten of leveranciers (bij gegevenslek);
- Tijd en datum van de ontdekking van het (vermoedelijke) gegevenslek of incident;
- Fysieke locatie van het gegevenslek of incident;
- Welke personen er nog op de hoogte zijn van het gegevenslek of incident;
- Welke acties u al heeft ondernemen tot zover (bijvoorbeeld computer disconnecteren van het internet of uitschakelen).

- Indien u een gegevenslek of incident heeft gemeld verwachten wij dat u bereikbaar bent in de loop van de dag zodat, indien nodig, acties zo snel als mogelijk kunnen genomen worden.

- Eindgebruikers die informatiesystemen en -diensten van Würth Belux gebruiken moeten elke geobserveerde of veronderstelde zwakheid in informatiesystemen of diensten ook melden.

2.6 Bewustzijn van werknemers en andere contractanten

Het **bewustzijn van werknemers en andere contractanten** creëren en continu verbeteren m.b.t. het verwerken van persoonsgegevens en informatieveiligheid moet gewaarborgd worden door:

- Het delen van dit privacybeleid bij de indiensttreding alsook het te publiceren op het intranet;

- Het voldoende communiceren omtrent privacy en informatieveiligheid in verschillende vormen, bijvoorbeeld via e-mail of op het intranet (nieuwsbrieven, voorbeelden, krantenartikels...);

- Het verplicht laten deelnemen van werknemers en contractanten aan infosessies & e-learning omtrent privacy en informatieveiligheid;

- Het laten evalueren van medewerkers omtrent de naleving van het privacybeleid.

2.7 Bijkomende technische en organisatorische maatregelen

Naast de bovenvermelde maatregelen, moeten de volgende **technische en organisatorische veiligheidsmaatregelen** geïmplementeerd, gevolgd en gecontroleerd worden om de persoonsgegevens voldoende te beschermen:

- Het steeds consulteren van de DPO bij de aanvang van nieuwe projecten of aanpassingen die een invloed kunnen hebben op het verwerken van persoonsgegevens en informatieveiligheid;

- Het bijhouden van de verzamelde persoonsgegevens mag enkel in een beveiligde fysieke en/of elektronische omgeving.

- Het slechts uitzonderlijk gebruiken van sterk-geëncrypteerde fysieke media (bv. usb-sticks) en meteen verwijderen na gebruik zodat de persoonsgegevens geen risico lopen op ongeoorloofde toegang;

- Het opruimen van de werkplek op het einde van de dag en confidentiële informatie (inclusief persoonsgegevens) veilig opbergen;

- Het steeds vergrendelen van de computer, laptop of Ipad bij het verlaten van het toestel;

- Het slechts (digitaal) kopiëren, doorsturen en afprinten van persoonsgegevens wanneer hier een echte noodzaak voor is. Na gebruik is het belangrijk om deze te vernietigen of te verwijderen;

- Het voorzichtig zijn met wachtwoorden: deel deze nooit met anderen ook niet met IT, schrijf deze niet op, vul geen wachtwoorden in indien anderen meekijken, gebruik verschillende wachtwoorden... Verander wachtwoorden bij een vermoeden als anderen het kennen. Gebruik een wachtwoordkluis zoals Keepass om al uw paswoorden te beheren.

- Het voorzichtig zijn met onbekende bestanden of hyperlinks in e-mails naar onbekende websites ter preventie van malware (virussen, spyware...). Verwittig de helpdesk steeds bij een vermoeden van malware.

3 Uitzonderingen

Indien u denkt dat er een noodzaak is voor een afwijking van dit privacybeleid, moet dit eerst worden gemeld en besproken met de DPO (privacy@würth.be) om het risiconiveau te bepalen. Pas daarna kan de uitzondering eventueel worden uitgevoerd mits een formele goedkeuring en eventuele maatregelen.

4 Gedragscode

Würth verwacht van alle werknemers en contractanten dat zij dit privacybeleid te allen tijde toepassen. Het niet naleven van de privacywetgeving (AVG-wetgeving 2016/679 (AVG/GDPR) is onderworpen aan disciplinaire maatregelen, zoals beschreven in het arbeidscontract van Würth. Gebruikers moeten zich ervan bewust zijn dat, op basis van toepasselijke wetten, het schenden van de privacy kan leiden tot strafrechtelijke of burgerlijke procedures.

Goedgekeurd op ....-....-201..

_____

CEO Würth Belux