

**Würth Belux**  
Privacy Management Systeem

**Privacybeleid**

Type de document :	Politique
Environnement :	Système de Privacy Management
Version :	V1
Date de création :	12/07/2018
Propriétaire du document :	
Classification	Usage interne
Dernière modification :	05/10/2018
Dernière révision :	Cliquez ici pour entrer une date
Approbation du management :	Cliquez ici pour entrer une date.
Remarques :	[Comments]


  
 A collection of handwritten signatures in blue ink, including:
 

- Smout
- S. Vermissen
- M. de Vos
- Lode Van de Velde
- Verheyen
- Polhuis
- Johan Vereecken
- Halvez St.
- P. Jansen
- Abasit
- Polhuis de Wit
- Arno Gebuch



## Informations relatives au document

---

### Clause de confidentialité

Toutes les informations reprises dans ce document sont classées en tant qu'informations à usage exclusivement interne et ne seront par conséquent accessibles qu'aux collaborateurs de Würth Belux (ci-après dénommé Würth). Les fournisseurs, contractants ... pourront accéder à ce document après avoir signé un contrat de confidentialité garantissant le respect de la politique, des normes et des procédures Würth en matière de vie privée et de protection des informations.

### Déclaration de conformité

Toute la documentation en matière de protection de la vie privée et des informations s'inspire des éléments juridiquement contraignants repris dans le contrat de travail Würth. Le cas échéant, les exigences légales et contractuelles y seront intégrées.

De façon générale, la documentation Würth en matière de protection des informations et de la vie privée constitue un ajustement et une extension des dispositions légales et contractuelles contraignantes s'appliquant à toute personne ayant accès à des informations Würth et utilisant, créant ou transformant ces informations.



# 1 Introduction

---

## 1.1 Objectif

Würth est parfaitement conscient du fait que son fonctionnement repose sur des données personnelles et que nous devons donc respecter et protéger la vie privée de toutes les personnes physiques, y compris des clients, des visiteurs du site Web, des collaborateurs, des fournisseurs et des autres tiers éventuellement concernés. Il convient de prendre les mesures qui s'imposent pour garantir notre conformité par rapport au RGPD et veiller à ce que les données personnelles soient protégées de toute utilisation, communication, modification ou destruction non autorisée, intentionnelle ou non. Le Data Protection Officer (DPO) est chargé du suivi du respect de cette politique.

## 1.2 Applicabilité

La présente politique de respect de la vie privée s'applique à l'ensemble du management, à tous les collaborateurs Würth (y compris les travailleurs temporaires) et à tout contractant traitant des données personnelles au nom de Würth (consultants et autres tiers).

## 1.3 Champ d'application

La présente politique de respect de la vie privée s'applique à toutes les activités professionnelles de Würth impliquant le traitement de données personnelles sous l'une ou l'autre forme.

## 1.4 Références

La présente politique de respect de la vie privée fait référence à la nouvelle législation RGPD/GDPR (2016/679) du Parlement Européen et du Conseil Européen ainsi qu'à la norme de protection des informations ISO27001:2013.

## 1.5 Définitions

<b>Personne concernée</b>	La personne physique dont les données personnelles sont traitées. Il peut s'agir de clients, de visiteurs du site Web, de collaborateurs, de fournisseurs ...
<b>Données personnelles</b>	Toutes les données relatives à une personne physique identifiée ou (indirectement) identifiable par le biais de tout support, y compris le courriel, les documents papier, l'instant messaging, les bases de données, les sites Web, les images vidéo, les enregistrements sonores, ...
<b>Données personnelles sensibles</b>	Certaines catégories de données personnelles exigeant un niveau de protection supérieur, en l'occurrence celles relatives à la race ou à l'origine ethnique, aux convictions religieuses ou philosophiques, à l'adhésion à un syndicat, aux opinions politiques, à la santé ainsi qu'aux faits répréhensibles supposés ou avérés.
<b>Traitements</b>	Activités couvrant la collecte, l'utilisation, le stockage, la modification, l'envoi, le transfert, la diffusion, la communication ou la suppression de données personnelles et relevant du domaine d'application de la présente politique.

## 2 Politique de protection de la vie privée

---

Les personnes concernées attendent de Würth que celui-ci collecte et utilise leurs données personnelles de manière légitime, conformément au RGPD. Les principes essentiels suivants servent de base permettant de vérifier si Würth répond à ces attentes et respecte bien le RGPD.

1. **La collecte et l'utilisation de données personnelles** doivent se faire de manière équitable et légale et uniquement à des fins légitimes ;
2. La collecte de données personnelles doit toujours se faire en **informant et en communiquant de façon suffisante avec la personne concernée** concernant le traitement de ses propres données personnelles ;
3. La **gestion des données personnelles** doit être conforme aux normes de qualité et aux délais de conservation prévus ;
4. Les **droits des personnes concernées** relatifs à leurs propres données personnelles doivent être respectés ;
5. Les **fuites de données personnelles** (supposées ou avérées) doivent être signalées et faire l'objet d'une enquête ;
6. Les **collaborateurs et autres contractants doivent être sensibilisés en permanence** à l'importance du traitement confidentiel des données personnelles ;
7. Il convient de prendre **des mesures de sécurité techniques et organisationnelles** afin de protéger les données personnelles.

### 2.1 Collecte et utilisation des données personnelles

Il convient de garantir **la collecte et l'utilisation** équitables et légales **des données personnelles** en prenant les mesures suivantes :

- Restriction de la collecte des données personnelles à ce qui exigé et autorisé, comme cela est prévu dans SAP, Speedy Touch, au niveau des supports de données et des autres modèles standard, le tout étant contrôlé par le DPO. La collecte de nombreuses autres données personnelles (par exemple des informations sur les membres de la famille d'un client) n'est pas autorisée.
- Respect du choix des prospects, des clients ... qui ne souhaitent pas être à nouveau contactés, y compris des clients ne souhaitant pas, par exemple, être contactés via Telesales.

- Respect de la décision d'un client qui retire son autorisation en matière de marketing par e-mail.

Remarque: Accountmanagers doivent utiliser une liste de diffusion dans un avenir prévisible pour respecter ces préférences. Ce sera encore communiqué.

- Collecte des données personnelles exclusivement à des fins légitimes ou lorsque cela est exigé par la loi. Les données personnelles collectées ne peuvent pas être utilisées à d'autres fins incompatibles ou à des fins autres que celles pour lesquelles elles l'ont été, sauf moyennant une demande d'autorisation en la matière ;
- Interdiction de partager des données personnelles avec des personnes externes, cela n'étant autorisé qu'en cas d'obligation légale (par exemple sur demande des autorités juridiques) ou si cela s'avère nécessaire pour répondre à des objectifs adéquats et légitimes et ce, en prenant toutes les garanties nécessaires (accord de non-divulgaration, contrat de transformateur). Il faut au préalable consulter le DPO ;
- Interdiction de transfert de données personnelles en dehors de l'Espace Économique Européen (EEE) sans analyse et approbation préalables du DPO.

## 2.2 Information et communication vis-à-vis de la personne concernée

**L'information et la communication nécessaires avec la personne concernée** relatives au traitement de ses propres données personnelles doivent être garanties par les éléments suivants :

- La documentation et la publication des déclarations de confidentialité nécessaires et spécifiquement élaborées pour les diverses personnes concernées (clients et collaborateurs (potentiels)) ;
- La mise à disposition aisée des déclarations de confidentialité, notamment sur le site Web pour les clients et sur l'intranet pour les collaborateurs ;
- La communication active de la déclaration de confidentialité par le biais d'un mail de confirmation automatique lors de l'enregistrement dans SAP, en se référant à la déclaration de confidentialité ;
- La communication active de la déclaration de confidentialité lors de l'entrée en service de nouveaux collaborateurs ;

- La référence verbale à la déclaration de confidentialité sur le site Web en cas de question portant sur le respect de la vie privée de la personne concernée ;
- La notification de la source lors de la première communication si les données personnelles ont été obtenues par d'autres sources que la personne concernée elle-même (par exemple Trendstop, BCE, LinkedIn).
- La mise à jour permanente des déclarations de confidentialité à partir des révisions périodiques et des modifications adéquates en cas de nouveaux traitements.

### 2.3 Gestion des données personnelles

La **gestion des données personnelles** au niveau interne et de façon conforme doit être garantie par les éléments suivants :

- Les données personnelles doivent être précises et exactes et si nécessaire mises à jour lorsqu'il n'y a plus eu de contact pendant une période d'environ deux ans. Cela peut se faire via notre site Web et nous comptons pour cela sur nos collaborateurs vérifieront les données personnelles lors du premier contact suivant ;
- On ne peut pas conserver les données personnelles plus longtemps que nécessaire pour répondre aux objectifs pour lesquels elles ont été collectées. Pour les prospects, cela correspond à un délai de maximum trois ans et, pour les clients, à un délai de maximum dix ans après le dernier achat. Pour les collaborateurs, cela correspond à un délai maximum de cinq ans après leur départ. Une fois ces différents délais expirés, toutes les données personnelles concernées seront (automatiquement) supprimées.

### 2.4 Droits des personnes concernées

Les **droits des personnes concernées** concernant leurs propres données personnelles doivent être respectés. Si un client souhaite exercer un droit, on doit le renvoyer à la déclaration de confidentialité reprise sur le site Web pour qu'il puisse contacter les personnes adéquates, sauf s'il s'agit du droit de modifier ses propres données personnelles. Ce droit peut être exercé par un collaborateur.

Les droits des personnes concernées couvrent ce qui suit :

- Le droit d'accès aux données personnelles conservées à son sujet,
- Le droit de correction de données personnelles inexactes ou incomplètes ;
- Le droit de suppression des données ou le droit à l'oubli ;
- Le droit d'arrêt du traitement de ses données personnelles ;
- Le droit de transférer ses données personnelles vers un autre responsable ;



- Le droit d'opposition au marketing direct et à toute utilisation de données personnelles ayant (ou pouvant avoir) des conséquences négatives pour la personne concernée ;
- Le droit de déposer plainte si l'on ne respecte pas sa vie privée.

Würth s'organise en la matière via la boîte de messagerie [privacy@wuerth.be](mailto:privacy@wuerth.be), mentionnée dans la déclaration de confidentialité reprise sur le site Web.

## 2.5 Notification de fuites de données

- Qu'est-ce qu'une fuite de données et un incident lié à la protection des informations ?
  - Une fuite de données est une situation dans laquelle des données personnelles risquent au minimum d'être publiées de façon non autorisée, d'être perdues, détruites ou modifiées. Une simple présomption suffit donc.
    - Exemples
      - Perte de dossiers « papier » contenant des données personnelles
      - Consultation non autorisée de documents ou de dossiers en ligne contenant des données personnelles
      - Perte d'une clé USB (ordinateur portable, GSM ...) cryptée de façon peu efficace (et contenant des données personnelles)
      - Erreur de destinataire externe d'un courriel contenant une liste de données personnelles en annexe
      - Partage de données personnelles sur Internet
      - Ordinateur, Ipad, ... piratés
    - Un incident de sécurité portant sur les informations concerne des données non personnelles (par exemple documents financiers ou stratégiquement importants). De tels incidents peuvent entraîner un préjudice en termes de réputation, une perte de confiance, des litiges et le non-respect d'exigences légales.
- Où dois-je signaler ces incidents ?
  - Vous devez signaler ce genre de faits le plus rapidement possible au helpdesk via les coordonnées suivantes :
    - [helpdesk@wuerth.be](mailto:helpdesk@wuerth.be)
  - Si vous estimez qu'il s'agit d'une fuite de données ou d'un incident critique susceptible d'affecter la réputation et la pérennité de Würth Belux, nous vous demandons de téléphoner le plus rapidement possible au helpdesk au numéro suivant :
    - 014/44.55.12
  - En cas de perte d'un ordinateur portable ou d'un Ipad, vous devez également prévenir systématiquement la police.
- Que dois-je signaler ?

- Si vous constatez une fuite de données ou un incident, vous devez le signaler immédiatement en fournissant les informations suivantes :
  - Vos propres coordonnées ;
  - Le fait qu'il s'agit d'une fuite de données ou d'un incident avéré ou si vous avez simplement des soupçons en la matière ;
  - Un bref descriptif de la fuite de données ou de l'incident (préssumé) :
    1. Le type de fuite de données ou d'incident ;
    2. Une estimation du nombre de personnes vers lesquelles les données ont fuité (en cas de fuite de données) ;
    3. À qui appartiennent les données, par exemple des collaborateurs, des clients ou des fournisseurs (en cas de fuite de données) ;
  - L'heure et le jour de la découverte de la fuite de données ou de l'incident (préssumé) ;
  - Le lieu physique de la fuite de données ou de l'incident ;
  - Les autres personnes qui sont également au courant de la fuite de données ou de l'incident ;
  - Les actions que vous avez déjà entreprises jusqu'à présent (par exemple déconnecter l'ordinateur d'Internet ou le débrancher).
  
- Si vous avez signalé une fuite de données ou un incident, nous escomptons que vous soyez joignable dans le courant de la journée afin que nous puissions, si nécessaire, entreprendre des actions le plus rapidement possible.
  
- Les utilisateurs finaux utilisant des systèmes et des services d'information Würth Belux doivent également signaler toute fragilité observée ou supposée des systèmes ou des services d'information.

## 2.6 Sensibilisation des collaborateurs et des autres contractants

Il convient de susciter et d'améliorer en permanence la **prise de conscience des collaborateurs et des autres contractants** en matière de traitement des données personnelles et de garantir la protection des informations grâce aux mesures suivantes :

- Partage de la présente politique de confidentialité lors de l'entrée en service ainsi que publication de cette politique sur l'intranet ;
- Communication suffisante en matière de protection de la vie privée et des informations sous différentes formes, par exemple par courriel ou sur l'intranet (lettres d'information, exemples, articles de journaux, ...) ;
- Participation obligatoire des collaborateurs et des contractants aux séances d'information et d'e-learning portant sur la protection de la vie privée et des informations ;

- Évaluation des collaborateurs en matière de respect de la politique de confidentialité.

## 2.7 Mesures techniques et organisationnelles complémentaires

Outre les mesures susmentionnées, il convient d'implémenter, de suivre et de contrôler les **mesures de sécurité techniques et organisationnelles** suivantes afin de protéger les données personnelles de façon suffisante :

- Consultation systématique du DPO au début de nouveaux projets ou d'adaptations susceptibles d'influencer le traitement de données personnelles et la protection d'informations ;
- La mise à jour des données personnelles collectées ne peut se faire que dans un environnement physique et/ou électronique sécurisé.
- Recours exceptionnel à des supports physiques cryptés de façon efficace (par exemple clés USB) et leur suppression immédiate après utilisation, afin que les données personnelles ne risquent pas de faire l'objet d'aucun accès non autorisé ;
- Le rangement du poste de travail en fin de journée et la mise en sécurité des informations confidentielles (y compris des données personnelles) ;
- Le verrouillage systématique de l'ordinateur, de l'ordinateur portable ou de l'ipad lorsque l'on quitte l'appareil en question ;
- La copie, la transmission et l'impression (numérique) de données personnelles uniquement lorsque cela correspond à une véritable nécessité. Il est important de détruire ces supports ou de les supprimer après utilisation ;
- Il convient d'être prudent avec les mots de passe : ne les partagez jamais avec d'autres personnes, même pas le département IT, ne les écrivez nulle part, ne complétez aucun mot de passe si d'autres personnes regardent l'écran en même temps que vous, utilisez plusieurs mots de passe différents, ... Changez de mot de passe si vous pensez que d'autres personnes risquent de l'avoir découvert. Utilisez un coffre-fort à mots de passe tel que Keeppass pour gérer tous vos mots de passe.
- Il convient de se montrer prudent avec les fichiers inconnus ou les hyperliens repris dans des courriels renvoyant vers des sites Web inconnus et ce, afin d'éviter l'irruption de logiciels malveillants (virus, logiciels-espions ...). Prévenez systématiquement le helpdesk en cas de suspicion de logiciel malveillant.



### 3 Exceptions

---

Si vous pensez qu'il est nécessaire de déroger à cette politique de confidentialité, vous devez tout d'abord le signaler et en discuter avec le DPO ([privacy@wuerth.be](mailto:privacy@wuerth.be)) afin de déterminer le niveau de risque correspondant. Ce n'est qu'ensuite que l'on pourra éventuellement faire exception à la règle, moyennant une approbation formelle et des mesures complémentaires éventuelles.

## 4 Code comportemental

---

Würth attend de tous ses collaborateurs et contractants qu'ils appliquent systématiquement et à tout moment la présente politique de confidentialité. Le non-respect de la législation en matière de respect de la vie privée (RGPD 2016/679 RGPD/GDPR) fera l'objet de mesures disciplinaires décrites dans le contrat de travail Würth. Les utilisateurs doivent être conscients du fait qu'en vertu des lois applicables, la violation de la vie privée peut générer des procédures pénales ou civiles.

Approuvé le ....-....-201..

---

CEO Würth Belux