État d'avancement de la conformité de TechIT.be en matière de protection des données à caractère personnel

Document destiné à la communication externe

TechIT.be
Siège social | Chaussée de Wavre 504 bte 48-1 – 1390 Grez-Doiceau
Numéro d'entreprise | 0849.350.806 - Numéro TVA | BE 0849.350.806
Site internet | https://www.techit.be/

Table des matières

État d'avancement de la conformité de TechIT.be en matière de protection des données à caractère personnel

1. Introduction

TechIT.be est une entreprise attachée au respect de la vie privée et accorde une grande importance à la protection des données à caractère personnel qu'elle est amenée à traiter dans le cadre de l'exécution de ses activités.

TechIT.be veille à traiter les données à caractère personnel de manière licite, loyale et transparente conformément aux dispositions légales applicables en la matière, dont le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après, le « RGPD ») et la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

Le présent document est destiné à informer les partenaires de TechIT.be de la manière dont elle envisage la protection des données à caractère personnel qu'elle traite dans le cadre de ses activités.

TechIT.be est pleinement consciente de la nécessité et de l'importance d'atteindre un niveau de conformité acceptable avec la réglementation relative à la protection des données à caractère personnel. C'est pour cette raison que l'organisation a fait appel à des organismes externes afin de l'aider à appréhender cette matière complexe et bénéficier d'une expertise dans ce domaine.

2. Conformité de TechIT.be

2.1. *Accountability*

En tant que responsable du traitement, TechIT.be prend les choses en main pour avancer vers un niveau de conformité en matière de protection des données adapté à sa réalité. Un comité de suivi des questions « RGPD » a notamment été mis en place au sein de TechIT.be. Ce comité comprend deux des administrateurs de l'organisation et la société Octogone Consulting SRL, cabinet de conseil spécialisé en protection des données qui accompagne TechIT.be dans sa mise en conformité RGPD. Ce comité se réunit plusieurs fois par an et fait le point sur les actions à mettre en œuvre afin de poursuivre le processus de conformité de TechIT.be

L'« *accountability* », basée sur le principe de responsabilité, implique la mise en œuvre active et continue de mesures par le responsable du traitement et les sous-traitants pour promouvoir et garantir la protection des données dans le cadre de leurs activités de traitement. Ce principe implique également une obligation pour le responsable du traitement et les sous-traitants de pouvoir démontrer à tout moment aux personnes concernées, au grand public et à l'autorité de contrôle la conformité avec les dispositions relatives à la protection des données

2.2. Principes généraux

Tant dans le cadre de sa gestion interne que dans ses activités professionnelles, TechIT.be veille à respecter les grands principes liés à la protection des données à caractère personnel (RGPD article 5). La Direction de TechIT.be est également consciente des enjeux entourant le **respect des principes de base du RGPD**.

L'article 5 du RGPD énonce, outre le principe de responsabilité vu ci-dessus (*accountability*), six principes qui régissent le traitement des données à caractère personnel. Ces principes sont expliqués ci-dessous :

Le Principe de licéité, loyauté et transparence : Premièrement, en vertu du principe de licéité, le traitement de données à caractère personnel doit être basé sur une des cinq bases de licéité prévues par l'article 6, §1 RGPD, à savoir, le consentement, le contrat, l'obligation légale, la mission d'intérêt public, l'intérêt légitime et la sauvegarde des intérêts vitaux. Deuxièmement, la loyauté signifie que la personne concernée doit être informée du risque afin de s'assurer que le traitement n'a pas d'effet négatif imprévisible. Troisièmement, les données doivent être traitées de manière transparente. La personne concernée doit être informée, en des termes clairs et simples, des finalités du traitement ainsi que de l'identité et l'adresse du responsable du traitement.

Le Principe de la limitation de la finalité qui implique que tout traitement doit être réalisé pour une finalité particulière bien définie.

Le Principe de minimisation des données qui implique que le traitement ne concerne que des données qui sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

Le Principe de l'exactitude des données qui implique que les données traitées doivent être exactes et tenues à jour.

Le Principe de la limitation de la durée de conservation qui implique que les données doivent être supprimées ou anonymisées dès qu'elles ne sont plus nécessaires pour les finalités pour lesquelles elles ont été collectées.

Le Principe d'intégrité et de confidentialité qui implique que les données doivent être traitées de façon à garantir une sécurité appropriée. Cela implique une protection contre le traitement non autorisé ou illicite mais également une protection contre la perte, la destruction ou les dégâts accidentels.

TechIT.be veille à prendre en compte tous ces principes lors des traitements de données à caractère personnel qu'elle opère.

2.3. Formation du personnel

L'article 32 du RGPD énonce les règles relatives à la sécurité du traitement. Selon cette disposition, le responsable du traitement doit prendre des mesures techniques et organisationnelles appropriées pour empêcher toute ingérence non autorisée dans le traitement de données. Dans ce contexte-là, des règles d'organisation internes peuvent être prises. C'est le cas lorsque le responsable du traitement met en place **des séances de sensibilisation et des formations continues des membres du personnel** concernant la sécurité et leurs obligations par rapport aux traitements de données à caractère personnel.

Au sein de TechIT.be, la Direction est consciente de l'importance de **sensibiliser les membres de son équipe**. En effet, le personnel bénéficie d'une formation continue concernant la cyber-résilience[1]. Par ailleurs, du fait de la nature des activités de TechIT.be, les travailleurs et la Direction sont naturellement plus sensibles aux questions en lien avec la sécurité de l'information. L'ensemble des formations continues est consigné dans un registre des sensibilisations, document interne permettant d'illustrer la conformité de TechIT.be.

[1] Formation fournie par l'organisme Phished (https://phished.io)

2.4. Sécurité

En vertu de l'article 32, §1 RGPD, le responsable du traitement doit prendre des mesures techniques et organisationnelles appropriées pour garantir la sécurité des traitements de données à caractère personnel. Les éléments repris dans la liste ci-après illustrent les **mesures techniques** mises en place en vue d'assurer la sécurité des traitements.

Dans ses activités métiers, TechIT.be tend à agir automatiquement de façon prudente et raisonnable. Sensibilisée à la problématique de la protection des données, l'organisation instaure des mesures techniques et organisationnelles assurant une certaine sécurité. En effet, TechIT.be veille à **traiter** les données de façon à garantir une **sécurité appropriée des données** à caractère personnel, notamment par les mesures suivantes citées de façon non-exhaustive :

- Installation de caméras de surveillance dans les locaux ;
- Gestion des accès logiques basés sur les rôles ;
- Gestion des mots de passes (2FA DUO) ;
- Gestion des mots de passes ponctuels via « one time password » ;
- Journalisation des logs ;
- Utilisation d'un gestionnaire de mots de passe ;
- Installation de BitLocker sur les machines ;
- Charte d'utilisation du matériel informatique ;
- Installation d'un anti-virus (fréquemment mis à jour) ;
- Installation d'un firewall (pare-feu) (fréquemment mis à jour) ;
- Mise en place d'un système de backup journalier ;
- Les clés USB et disques durs externes et contenant des données personnelles sont interdits (sauf s'ils sont protégés par un système de cryptage) ;
- Les données à caractère personnel sont encryptées ;
- Tous les logiciels sont mis à jour systématiquement et automatiquement ;
- Connexion sécurisée par SSL (HTTPS) du site internet ;
- Détection de tout accès non autorisé ou utilisation anormale est mis en place en interne ;
- Utilisation systématiquement du chiffrement (cryptage) sur le réseau et les appareils mobiles ;
- Installation de défenses anti-malware ;
- Présence d'un système de détection ou de prévention d'intrusion sur le réseau ;
- Wi-Fi protégé par un mot de passe complexe ;
- Mise en place des mesures de contrôle des communications électroniques des travailleurs ;
- …

2.5. Délégué à la protection des données

TechIT.be a désigné un **DPO externe**. Cette mission à été confiée à la société Octogone consulting srl, spécialiste en protection des données. Cette désignation a été notifiée en bonne et due forme à l'Autorité belge de protection des données (APD). Octogone, en qualité de cabinet spécialisé, se spécialise et se forme continuellement.

Le DPO, ou Délégué à la Protection des Données, est un acteur clé dans le domaine de la protection des données à caractère personnel au sein d'une organisation. Sa mission principale consiste à veiller à la conformité des activités de traitement des données avec les réglementations en vigueur, telles que le Règlement Général sur la Protection des Données (RGPD).

Le rôle du DPO s'étend au-delà de la simple conformité, englobant également la sensibilisation et la formation des employés sur les enjeux liés à la confidentialité des données. Il doit être le point de contact privilégié tant pour l'autorité de contrôle que pour les individus concernés, assurant un appui et une communication transparente et rapide en cas de violation de données.

En résumé, le DPO incarne un pilier crucial dans la préservation des données à caractère personnel et de la confidentialité des données au sein des organisations, assurant ainsi une culture de protection des données robuste et conforme aux normes législatives en vigueur.

2.6. Registre des activités de traitement

TechIT.be s'est doté d'un **registre des activités de traitement**. Une première version de registre a été élaborée et est en cours de révision. Le registre des activités de traitement est un outil central de conformité qui permet de répondre à d'autres obligations découlant du RGPD.

Un registre des activités de traitement est un document clé en matière de protection des données personnelles. Ce registre recense et détaille toutes les activités de traitement des données à caractère personnel au sein d'une organisation.

Essentiellement, ce registre remplit plusieurs fonctions cruciales. Tout d'abord, il identifie clairement qui est responsable du traitement des données et s'il y a des sous-traitants impliqués. Ensuite, il spécifie les finalités du traitement, c'est-à-dire les raisons pour lesquelles les données personnelles sont traitées. Cela peut englober divers domaines tels que la gestion des ressources humaines, la relation avec les clients, la facturation, etc.

Le registre détaille également les catégories de données personnelles traitées, telles que les noms, adresses, numéros de téléphone, adresses e-mail, etc. Il identifie les catégories de personnes concernées, que ce soient des employés, des clients, des fournisseurs, ou d'autres parties prenantes. Pour assurer la transparence et la conformité, le registre mentionne également les éventuels transferts de données en dehors de l'Union européenne, en précisant les destinations et les garanties de protection mises en place. De plus, il spécifie la durée de conservation des données, indiquant combien de temps les informations personnelles seront conservées.

En matière de sécurité, le registre décrit les mesures mises en place pour protéger les données, assurant ainsi un traitement responsable et sécurisé. Si une organisation dispose d'un délégué à la protection des données (DPO), ses coordonnées sont également incluses dans le registre.

En résumé, le registre des activités de traitement constitue un outil indispensable pour aider les organisations à démontrer leur conformité avec les normes de protection des données, garantissant une gestion transparente des données personnelles.

3. Garanties apportées par TechIT.be concernant le traitement des demandes d'exercice de droit et des violations de données

3.1. Gestion des demandes d'exercice de droit

TechIT.be s'engage à traiter avec diligence **les demandes d'exercice de droits** qu'elle recevrait de la part d'une personne concernée, et au besoin elle pourra s'adresser à son DPO qui pourra l'aider dans la gestion des demandes d'exercice qu'elle recevrait. En effet, TechIT.be est pleinement consciente que le RGPD confère certains droits à la personne dont les données sont traitées.

Les personnes concernées peuvent exercer les droits suivants :

Le droit d'accès c'est-à-dire le droit pour les personnes d'accéder à leurs propres données et d'obtenir certaines informations sur le traitement. Lorsque la personne concernée en fait la demande, le responsable du traitement doit fournir une copie des données faisant l'objet d'un traitement. La communication doit par ailleurs se faire sous une forme compréhensible.

Le droit de rectification c'est-à-dire le droit pour les personnes de faire rectifier leurs données par le responsable du traitement si elles sont inexactes. Le considérant 65 du Règlement indique par ailleurs que l'exactitude des données à caractère personnel est essentielle pour garantir un niveau élevé de protection.

Le droit à l'effacement c'est-à-dire le droit de faire effacer ses données dans les meilleurs délais. Le droit à l'effacement, inscrit dans le Règlement général sur la protection des données, confère aux individus le pouvoir de demander la suppression de leurs données personnelles par les responsables du traitement. Ce droit s'applique dans divers contextes tels que la non-nécessité des données au regard de la finalité, le retrait du consentement ou encore l'opposition au traitement. Toutefois, il peut être restreint dans certaines situations, notamment en cas d'obligations légales ou d'exercice du droit à la liberté d'expression.

Le droit à la limitation du traitement autorise les individus à restreindre temporairement le traitement de leurs données personnelles par le responsable. Ce droit peut être invoqué dans plusieurs circonstances, telles que la contestation de l'exactitude des données, l'illicéité du traitement ou encore le besoin de conserver les données pour la défense de droits en justice. Contrairement au droit à l'effacement, la limitation n'entraîne pas la suppression des données, mais plutôt leur mise en quarantaine jusqu'à résolution du litige ou de la situation conflictuelle.

Le droit à la portabilité c'est-à-dire le droit d'obtenir ses données à caractère personnel et de les réutiliser pour d'autres services. Lorsque le traitement des données fournies est d'une part, effectué à l'aide de procédés automatisés et d'autre part, fondé sur le consentement. Ou lorsque le traitement est nécessaire à l'exécution d'un contrat et est effectué à l'aide de procédés automatisés. Dans ces cas-là, la personne concernée a le droit d'obtenir que leurs données soient transmises directement d'un responsable de traitement à un autre, si cela est techniquement possible.

Le droit d'opposition confère aux individus le pouvoir de s'opposer au traitement de leurs données personnelles par le responsable du traitement. Ce droit peut être exercé à tout moment et pour des raisons liées à la situation particulière de la personne, notamment en cas de marketing direct, de profilage, ou lorsque le traitement est fondé sur l'exécution d'une mission d'intérêt public ou d'exercice de l'autorité publique. Le responsable du traitement doit alors cesser de traiter les données, à moins qu'il ne démontre des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts, les droits et les libertés de la personne concernée, ou pour l'établissement, l'exercice ou la défense de droits en justice.

3.2 Les violations de données

En cas de **violations de données à caractère personnel**, tels qu'un incident de sécurité compromettant l'intégrité, la confidentialité ou la disponibilité des données à caractère personnel, Tech IT.be réagira, de manière appropriée afin d'atténuer les éventuels préjudices et afin de faire cesser cette violation. Par ailleurs, TechIT.be évaluera l'étendue des risques et n'hésitera pas à solliciter l'avis et les conseils de son DPO.

L'article 4, §12 RGPD définit la violation de données à caractère personnel comme étant une violation de la sécurité, entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel traitées ou l'accès non-autorisé à de telles données. Afin de limiter les conséquences des violations de données, le RGPD impose une obligation de notification à l'autorité de contrôle et à la personnes concernées dans certaines circonstances.

Une violation de données se produit lorsqu'il y a un accès non autorisé, une divulgation, une perte ou une altération non intentionnelle de données personnelles. Cela peut inclure tout, depuis le vol de données jusqu'à la perte d'un dispositif contenant des informations confidentielles. Le Règlement général sur la protection des données impose au responsable du traitement de notifier les violations de données à l'autorité de contrôle compétente dans les 72 heures après en avoir pris connaissance, sauf si la violation ne présente pas de risque pour les droits et les libertés des personnes concernées. Si la violation présente un risque élevé pour ces droits, les personnes concernées doivent également être informées.

En cas de violation de données, le responsable du traitement doit prendre des mesures immédiates pour remédier à la situation, limiter les impacts, et prévenir de futures violations. La notification à l'autorité de contrôle et, le cas échéant, aux personnes concernées, doit inclure des détails sur la nature de la violation, les catégories et le nombre d'individus affectés, les conséquences potentielles, et les mesures prises pour remédier à la situation. Les entreprises peuvent être soumises à des amendes en cas de non-conformité avec ces obligations. Il est essentiel de mettre en place des procédures internes et des mesures de sécurité pour prévenir et gérer efficacement les violations de données conformément aux exigences du RGPD.

4. Conclusion

Dans le cadre de son **processus de mise en conformité continu**, la Direction de TechIT.be s'est engagée à mettre en œuvre des procédures et mécanismes qui lui permettront d'améliorer sa conformité continuellement. En travaillant de concert avec son DPO, l'organisation organise régulièrement des réunions de suivi durant lesquelles elle définit les actions à mettre en œuvre prioritairement pour se conformer aux règles du RGPD.

Ainsi, TechIT.be s'est dotée d'un Plan d'action établi avec l'aide de son DPO, afin de cibler toutes les actions à mettre en œuvre à l'avenir pour améliorer sa conformité. Ce plan d'actions identifie par ailleurs certaines actions prioritaires à mettre en œuvre rapidement. Citons par exemple : Continuer à formaliser la documentation RGPD de TechIT.be ; Élaborer un dossier RGPD que TechIT.be pourra fournir aux clients qui en font la demande afin d'illustrer sa conformité au RGPD ; Encadrer les relations entre TechIT.be et ses freelances (sous-traitants) ; Améliorer le registre des activités de traitement que TechIT.be possède déjà ; …

Pour plus d'informations concernant la conformité de TechIT.be, n'hésitez pas à vous adresser aux membres du Comité de suivi des questions RGPD, Dimitri Rolin (dimitri.rolin@techit.be) et Antoine Waterkeyn (antoine.waterkeyn@techit.be).

* *

*

Grez-Doiceau, le 1 février 2024,

Dimitri Rolin et Antoine Waterkeyn