proximus

DPO

Protection des données et secret des communications électroniques

Last update on 25/07/2023
Owner Data Protection Officer

Table des matières

1. Introduction

1.1 Objectif de la politique

Le Groupe Proximus s'engage à respecter l'ensemble de la législation pertinente en matière de protection des données et les bonnes pratiques relatives au traitement des données de communications électroniques et des données personnelles, comme indiqué dans la présente politique.

Une raison importante pour traiter les données de communications électroniques et les données personnelles avec une stricte confidentialité est que ces données sont légalement protégées. Tout manquement des entités du Groupe Proximus ou de leurs employés, contractants et représentants à ces obligations légales peut faire l'objet de sanctions pénales, administratives et disciplinaires.

Il va sans dire que le respect de la confidentialité des communications électroniques et de la vie privée de nos clients est essentiel si nous voulons gagner et conserver les clients et leur confiance.

Le Groupe Proximus s'engage à respecter toutes les législations pertinentes en matière de données personnelles et à protéger les droits et libertés des personnes conformément, entre autres, au Règlement général sur la protection des données (**RGPD**[1]) et à la directive vie privée et communications électroniques (**Directive e-Privacy**[2]), transposée dans la législation belge par la loi sur les communications électroniques du 13/06/2005.

1.2 Champ d'application de la politique

La présente politique s'applique à tous les employés et (sous-)contractants du Groupe Proximus et à tout traitement de données personnelles[3], y compris les données de communications électroniques[4], par le Groupe Proximus, que ce soit en tant que responsable du traitement ou en tant que sous-traitant[5]. Ceci inclut les données personnelles de toutes les catégories suivantes de personnes concernées[6] : les clients actifs de Proximus ainsi que les données des prospects et des anciens clients et les données des candidats, les employés et (sous-)contractants actuels de Proximus et les anciens employés et (sous-)contractants de Proximus et s'applique aussi bien aux clients résidentiels qu'aux clients professionnels.

Les employés du Groupe Proximus, mais aussi les (sous-)contractants et tous les tiers qui travaillent avec ou pour le Groupe Proximus et qui ont ou peuvent avoir accès à des données personnelles, sont censés avoir lu et compris la présente politique et s'y conformer. Veuillez noter que dans la suite de la présente politique, le terme "employé de Proximus" couvre à la fois les employés et les (sous-)contractants du Groupe Proximus.

[1] Voir la définition de « RGPD » à l'Annexe 1.
[2] Voir la définition de « Directive e-Privacy » à l'Annexe 1.
[3] Voir la définition de « données personnelles » à l'Annexe 1.
[4] Voir la définition de « donnée de communications électroniques » à l'Annexe 1.
[5] Voir les définitions de « responsable du traitement » et de « sous-traitant » à l'Annexe 1.
[6] Voir la définition de « personne concernée » à l'Annexe 1.

La présente politique est conforme au RGPD et à la Directive e-Privacy.

Le RGPD s'applique à tous les responsables du traitement qui sont établis dans l'Union européenne (**UE**) et qui traitent les données personnelles de personnes concernées, dans le cadre de cet établissement[7]. Il s'applique également aux responsables du traitement hors de l'UE qui traitent les données personnelles de personnes concernées qui se trouvent dans l'UE, lorsque les activités de traitement sont liées :

- à l'offre de biens ou de services à ces personnes concernées dans l'UE, qu'un paiement soit exigé ou non desdites personnes ; ou
- au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'UE.

1.3 Que doivent faire les employés de Proximus ?

La présente section vise à donner un aperçu des points d'action que les employés de Proximus doivent prendre pour se conformer aux obligations de la présente politique. La liste ci-dessous n'est pas exhaustive et vise simplement à mettre en évidence les exigences les plus importantes sous une forme concrète.

1.3.1 Appliquer les principes du traitement des données personnelles à la collecte et à l'utilisation de données personnelles

- Ne collecter que les données personnelles qui sont directement pertinentes et nécessaires pour atteindre le(s) but(s) spécifié(s) et ne conserver les données personnelles que pour la durée nécessaire pour atteindre le(s) but(s) spécifié(s).
- Utiliser les données personnelles uniquement pour les finalités pour lesquelles elles ont été collectées.
- Veiller à ce que les données personnelles soient exactes, à jour et pertinentes au regard de la ou des finalités pour lesquelles elles sont collectées.
- Protéger les données personnelles (papier et électroniques) par des mesures de sécurité appropriées contre des risques tels que la perte, l'accès ou l'utilisation non autorisés, la destruction, la modification ou la divulgation involontaire ou inappropriée.
- Éviter d'accéder, de collecter ou de stocker des données personnelles qui ne sont pas nécessaires dans le cadre de leurs responsabilités professionnelles actuelles.
- Détruire les données personnelles en toute sécurité lorsqu'elles ne sont plus nécessaires pour atteindre les finalités spécifiées.

1.3.2 Suivez la procédure de « privacy by design »

- Suivre la procédure de « privacy by design »[8] lors de la phase initiale de conception de tout système, produit ou processus impliquant le traitement de données personnelles.

[7] Voir la définition d' « établissement » à l'Annexe 1.
[8] Le processus de « privacy by design » est un processus mis en place pour prendre en compte les obligations en matière de protection des données lors de la conception de toute initiative impliquant le traitement de données personnelles. Voir la section 2.3.

- Mettre en œuvre les mesures définies dans le cadre de la procédure de « privacy by design » pour atténuer les risques que cette activité de traitement peut présenter pour les droits et libertés des personnes physiques.

1.3.3 Signaler les violations de données personnelles et les plaintes

- Informer immédiatement le Data Protection Office lorsqu'une violation de données personnelles est détectée. Une violation de données personnelles se produit lorsque la confidentialité, la disponibilité ou l'intégrité de données personnelles est compromise.
- Signaler au Data Protection Office toute plainte émanant d'une personne concernée sur la manière dont ses données personnelles sont traitées.

1.3.4 Compléter les formations requises

- Suivre et terminer toutes les formations requises en matière de protection des données et de sécurité de l'information.

2. Politique : protection des données

2.1 Conséquences en cas de non-conformité

2.1.1 RGPD

Le RGPD est entré en vigueur le 25 mai 2018. Il n'y a pas de dispositions transitoires pour les données personnelles existantes. Cela signifie que, à partir de cette date, le Groupe Proximus doit se conformer entièrement au RGPD.

Le Groupe Proximus exerce des activités de traitement pour lesquelles il se qualifie de responsable de traitement et des activités pour lesquelles il se qualifie de sous-traitant en vertu du RGPD et risque des sanctions en cas de non-respect de ses obligations en vertu de la législation sur la protection des données.

Le RGPD prévoit différents types de sanctions en cas de non-respect des règles de protection des données, notamment des réprimandes, des interdictions temporaires ou définitives de traiter des données personnelles et des amendes pouvant atteindre 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise.

2.1.2 Loi du 13/06/2005 relative aux communications électroniques

Les sanctions possibles en cas de non-respect de la Directive e-Privacy sont prévues à la section 3.3.

2.1.3 Actions disciplinaires

Toute violation de la présente politique peut entraîner des mesures disciplinaires pouvant aller jusqu'au licenciement, conformément à la réglementation du travail qui vous est applicable. Les violations de la

législation sur la protection des données peuvent également constituer une infraction pénale, auquel cas l'affaire sera signalée dès que possible aux autorités compétentes.

2.2 Principes du traitement des données personnelles

Tout traitement de données personnelles doit être effectué conformément aux principes de protection des données suivants. Tout nouveau produit ou service impliquant le traitement de données personnelles doit suivre la procédure de « privacy by design » afin de s'assurer que ces principes sont pris en compte lors de sa conception.

2.2.1 Licéité, loyauté et transparence

Les données personnelles doivent être traitées de manière licite, loyale et transparente.

2.2.1.1 Licéité

Les données à caractère personnel doivent être traitées de manière licite. Pour que le traitement soit considéré comme licite, il doit être fondé sur l'une des bases juridiques énumérées à l'article 6.1 du RGPD, à savoir :

- Consentement préalable de la personne concernée ;
- Exécution d'un contrat ;
- Respect d'une obligation légale du responsable du traitement ;
- Protection de l'intérêt vital de la personne concernée ;
- Exercice de l'intérêt public ou d'une autorité officielle ; ou
- Intérêt légitime de Proximus ou d'un tiers.

Il n'y a pas de hiérarchie entre les bases juridiques ci-dessus.

Une base juridique spécifique est nécessaire pour traiter des catégories particulières de données personnelles[9].

La licéité signifie également que le traitement des données personnelles ne doit pas être illégal ou illicite d'une manière plus générale. Cela implique que toute activité de traitement doit respecter les lois et principes pénaux et civils applicables.

La base juridique appropriée pour une activité de traitement est définie et documentée dans le cadre de la procédure de « privacy by design » qui doit être suivi pour toute nouvelle initiative impliquant le traitement de données personnelles.

[9] Voir la définition de « catégories particulières de données personnelles » à l'Annexe 1.

2.2.1.2 Loyauté

Le traitement des données personnelles doit être loyal. Cela signifie que :

- Le Groupe Proximus traite les données personnelles d'une manière à laquelle les personnes concernées peuvent raisonnablement s'attendre (transparence et attentes raisonnables) ;
- Le Groupe Proximus n'utilise pas les données personnelles de manière à porter préjudice aux personnes concernées ;
- Le Groupe Proximus ne trompe pas les personnes concernées ;
- Le Groupe Proximus n'incite pas les personnes concernées à accepter le traitement de leurs données personnelles.

2.2.1.3 Transparence

Le RGPD impose des obligations accrues quant aux informations qui doivent être mises à la disposition des personnes concernées, celles-ci étant comprises dans l'obligation de « transparence ». Il définit quelles informations relatives au traitement des données personnelles doivent être fournies aux personnes concernées, ainsi que quand et comment ces informations doivent être fournies.

Le contenu obligatoire des informations qui doivent être fournies aux personnes concernées est défini par les articles 13.1 et 13.2 ou 14.1 et 14.2 du RGPD.

Les informations et communications relatives au traitement des données personnelles doivent être :

- concises, transparentes, intelligibles et facilement accessibles ;
- dans un langage clair et simple ;
- par écrit ou par d'autres moyens, y compris, le cas échéant, par des moyens électroniques ; et
- fournies gratuitement.

Les informations relatives au traitement des données personnelles doivent être fournies aux personnes concernées dans le délai prévu par les articles 13.1 et 14.3 (a) à (c) du RGPD.

2.2.2 Limitation des finalités

Les données personnelles ne sont collectées et traitées que pour des finalités déterminées, légitimes et explicites et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités. Au cours de la procédure de « privacy by design », il est vérifié et documenté si un traitement de données personnelles est justifié par une finalité valable ou si une nouvelle finalité est compatible avec la finalité initiale du traitement.

2.2.2.1 Spécification de la finalité

La finalité du traitement des données personnelles doit être établie au préalable et déterminée au moment de la collecte ou du traitement ultérieur des données personnelles.

Si l'activité de traitement ne répond à aucune finalité spécifique, elle ne doit pas avoir lieu ou doit être suspendue immédiatement lorsque la finalité devient inexistante.

2.2.2.2 Finalité légitime

Une finalité légitime est une finalité qui répond à toutes les exigences légales. En outre, une finalité légitime est une finalité valable. Non seulement elle doit être licite, mais elle doit également être raisonnable et réaliste.

2.2.2.3 Finalité explicite

Une finalité explicite est une finalité qui est clairement révélée, expliquée et exprimée. La finalité doit être explicite au plus tard au moment où les données personnelles sont collectées ou traitées ultérieurement.

2.2.2.4 Utilisation compatible

Les données personnelles obtenues pour des finalités déterminées ne doivent pas être utilisées ultérieurement pour une autre finalité qui ne serait pas compatible avec la finalité initialement définie. Néanmoins, il est permis de traiter des données personnelles pour une nouvelle finalité dans les cas où les données ont été collectées sur la base d'un intérêt légitime, d'un contrat ou d'intérêts vitaux, mais seulement après avoir vérifié que la nouvelle finalité est compatible avec la finalité initiale.

2.2.3 Minimisation des données

Les données personnelles doivent être adéquates (suffisantes pour atteindre la finalité spécifiée), pertinentes (présentant un lien rationnel avec cette finalité) et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

Si certaines données personnelles ne sont pas strictement nécessaires à la finalité en question, elles ne peuvent être collectées ou traitées.

Les méthodes de collecte des données sont examinées dans le cadre de la procédure de « privacy by design » afin de s'assurer que les données collectées sont adéquates, pertinentes et non excessives.

2.2.4 Exactitude

Les données personnelles doivent être exactes et tenues à jour.

Afin d'obtenir une précision optimale, les données personnelles doivent, dans la mesure du possible, être obtenues auprès des personnes concernées elles-mêmes. Les données personnelles qui sont conservées par le Groupe Proximus doivent être passées en revue et mises à jour si nécessaire.

2.2.5 Limitation de la conservation

Les données personnelles doivent être conservées sous une forme permettant d'identifier la personne concernée uniquement pendant la durée nécessaire aux finalités pour lesquelles elles sont traitées. Les données personnelles ne peuvent être conservées pour une durée indéterminée. La durée de la conservation peut varier en fonction de la finalité pour laquelle les données personnelles sont traitées. Pendant toute la durée de conservation, le Groupe Proximus doit être en mesure de prouver que la conservation des données personnelles est nécessaire pour atteindre cette finalité.

La durée de conservation appropriée des données personnelles est définie et documentée dans le cadre de la procédure de « privacy by design » qui doit être suivi pour toute nouvelle initiative impliquant le traitement de données personnelles.

Le Groupe Proximus doit veiller à ce que les données personnelles soient anonymisées, supprimées ou détruites de manière sécurisée à la fin de leur période de conservation.

2.2.6 Sécurité des données personnelles

Les données personnelles doivent être traitées de manière à garantir une sécurité appropriée des données personnelles, notamment une protection contre le traitement non autorisé ou illégal et contre la perte, la destruction ou les dommages accidentels, au moyen de mesures techniques ou organisationnelles appropriées. Le Groupe Proximus met en œuvre les mesures techniques et organisationnelles nécessaires pour assurer une sécurité adéquate des données personnelles.

Toutes les données personnelles sont classées et traitées en fonction de leur niveau de sensibilité, tel que défini dans la politique de propriété et de classification des informations de Proximus.

Lors de l'évaluation des mesures visant à garantir une sécurité appropriée des données personnelles, une évaluation des risques sera effectuée en tenant compte de toutes les circonstances des activités de traitement du Groupe Proximus ainsi que de l'étendue des dommages ou des pertes qui pourraient être causés aux personnes concernées en cas de violation de la sécurité, de l'effet de toute violation de la sécurité sur le Groupe Proximus lui-même et de tout dommage probable à la réputation, y compris la perte éventuelle de la confiance des clients.

Lors de l'évaluation des mesures techniques appropriées, les mesures suivantes seront notamment prises en compte :

- Ségrégation réseau (firewalls et passerelles internet) ;
- Techniques permettant d'accroître la protection de la vie privée telles que la pseudonymisation et l'anonymisation ;
- Gestion des identités et des accès (infrastructure à clé publique, infrastructure de gestion de clés, etc.) ;
- Gestion des menaces et vulnérabilités (scan et correction des vulnérabilités, enregistrement et surveillance des événements, protection contre les logiciels malveillants, détection des intrusions, etc.) ;
- Protection contre la perte de données ;
- Gestion du chiffrement ;
- Sécurité des applications (sécurité SOA, sécurité des bases de données, etc.) ;
- Protection des composants réseau et des appareils des utilisateurs finaux ;
- Security Information & Event Management ;
- Séparation données, applications et réseau ;
- Logs d'audit et monitoring ;
- Gestion de l'accès à distance des fournisseurs et tiers.

Lors de l'évaluation des mesures organisationnelles appropriées, les mesures suivantes seront notamment prises en compte :

- Politiques de protection des données ;
- Formation et sensibilisation des employés de Proximus ;
- Contrôles d'accès physique ;
- Adoption d'une politique « clear desk ».

Tous les employés de Proximus sont tenus de veiller à ce que les données personnelles dont dispose le groupe Proximus et dont ils sont responsables restent sécurisées.

2.2.6.1 Intégrité

Les données personnelles doivent être correctement sécurisées afin de garantir leur intégrité. L'intégrité des données doit être prise en compte tout au long du cycle de vie de tout projet ou processus.

2.2.6.2 Confidentialité

Les données personnelles peuvent uniquement être consultées par des personnes qui en ont besoin, comme le stipule le principe du « need to know » : l'accès aux données personnelles doit toujours être limité aux personnes pour lesquelles ces données sont nécessaires à l'exécution de leurs tâches. Le Groupe Proximus doit veiller à ce que les données personnelles ne soient traitées que par des employés ou des équipements autorisés.

2.2.7 Responsabilité

En tant que responsable du traitement, conformément à l'article 5.2 du RGPD, le Groupe Proximus est non seulement chargé d'assurer la conformité avec le RGPD, mais aussi de démontrer que ses activités de traitement sont conformes aux principes du traitement des données énumérés dans la présente politique et aux obligations du RGPD (**principe de responsabilité**).

Afin de pouvoir démontrer sa conformité, le Groupe Proximus conservera une documentation de chaque décision prise et mesure mise en œuvre pour se conformer aux principes du traitement des données énoncés dans la présente politique, y compris en mettant en œuvre une procédure de « privacy by design », en tenant des registres d'activités de traitement, en exécutant et en documentant des DPIA lorsque la loi l'exige, en mettant en œuvre et en documentant des mesures de sécurité techniques et organisationnelles, en mettant en œuvre un processus de notification de violations des données personnelles, en facilitant l'exercice des droits des personnes concernées, etc. Cette documentation sera mise à la disposition de l'autorité de contrôle sur demande et sert de preuve du respect de la réglementation en matière de protection des données.

En matière de contrôle de la conformité, Proximus applique le système décrit à la section 4 de la présente politique.

2.3 Procédure de « privacy by design »

Conformément au principe de responsabilité du RGPD[10], le Groupe Proximus doit être en mesure de démontrer sa conformité à la réglementation sur la protection des données (par exemple, le RGPD, la

[10] Le principe de responsabilité est expliqué à la section 2.2.7.

Directive e-Privacy) et s'assurer que le traitement des données personnelles est conforme à la législation applicable.

Le Groupe Proximus doit établir une procédure (**procédure de « privacy by design »**) pour vérifier la conformité aux obligations de la réglementation sur la protection des données pour toute initiative impliquant le traitement de données personnelles. La procédure de « privacy by design » permet au Groupe Proximus d'anticiper et de mitiger les risques et les événements portant atteinte à la vie privée avant qu'ils ne se produisent, garantissant ainsi la mise en œuvre correcte des principes de protection des données. La procédure de « privacy by design » garantit également qu'au cours de la phase initiale de conception de tout système, produit ou processus, le Groupe Proximus prenne en compte les points suivants :

- La conformité des activités de traitement des données personnelles prévues aux principes de protection des données ;
- Les risques que ces activités de traitement peuvent présenter pour les droits et libertés des personnes physiques ; et
- Les éventuelles mesures disponibles pour mitiger les risques et démontrer sa conformité à la législation.

2.4 Data Protection Impact Assessment

Le Groupe Proximus procède à une analyse de l'impact des opérations de traitement envisagées sur la protection des données personnelles dès lors qu'une activité de traitement est susceptible d'entraîner un risque élevé pour les droits et libertés des personnes. Cette analyse est appelée analyse d'impact sur la protection des données ou « Data Protection Impact Assessment » en anglais (**DPIA**).

Un DPIA est requis au moins dans les cas suivants :

- l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, y compris le profilage, et sur la base de laquelle ;
- le traitement à grande échelle de données sensibles ;
- la surveillance systématique à grande échelle d'une zone accessible au public ;
- le traitement à grande échelle et/ou systématique de données de téléphonie, d'Internet ou d'autres données de communication, de métadonnées ou de données de localisation de personnes physiques ou permettant de mener à des personnes physiques (par exemple le wifi-tracking ou le traitement de données de localisation de voyageurs dans les transports publics) lorsque le traitement n'est pas strictement nécessaire pour un service demandé par la personne concernée.

Les DPIA doivent contenir et documenter au moins les éléments obligatoires énumérés à l'article 35.7 du RGPD.

2.5 Droits des personnes concernées

Les personnes concernées ont les droits suivants à l'égard du traitement de leurs données personnelles :

- Droit d'être informé
- Droit d'accès
- Droit de rectification
- Droit à l'effacement (**droit à l'oubli**)
- Droit à la limitation du traitement
- Droit à la portabilité des données
- Droit d'opposition

- Droits liés à la prise de décision automatisée et au profilage

Le Groupe Proximus élabore et maintient des procédures et des formations appropriées pour mettre en œuvre les droits des personnes concernées susmentionnés et pour traiter les plaintes des personnes concernées sur la manière dont leurs données personnelles ont été traitées par le Groupe Proximus.

Le Groupe Proximus doit mettre à la disposition des personnes concernées les moyens appropriés pour leur permettre d'exercer leurs droits et d'introduire leurs plaintes.

Lorsque la loi l'exige, le Groupe Proximus doit exécuter la demande de la personne concernée et y répondre dans le délai prévu à l'article 12.3 du RGPD.

2.6 Consentement

Comme expliqué dans la section 2.2.1.1 de la présente politique (**principe de licéité**), le traitement des données personnelles doit être fondé sur l'une des bases juridiques énumérées dans le RGPD. L'une de ces bases juridiques est le consentement préalable de la personne concernée. Chaque fois que le traitement des données personnelles est fondé sur cette base juridique, des exigences supplémentaires doivent être respectées pour que le consentement soit valable.

Pour être valable, le "consentement" doit être collecté sous la forme d'une indication libre, spécifique, informée et non équivoque de la volonté de la personne concernée par laquelle celle-ci, par une déclaration ou par une action positive claire, marque son accord pour le traitement des données personnelles la concernant. Le consentement de la personne concernée peut être retiré à tout moment.

Pour obtenir un consentement valable, la personne concernée doit avoir été pleinement informée du traitement envisagé et avoir marqué son accord, tout en étant dans un état d'esprit apte à le faire et sans qu'aucune pression ne soit exercée sur elle. Le consentement obtenu sous la contrainte ou sur la base d'informations trompeuses ne constituera pas une base valable pour le traitement. Le consentement ne peut être déduit de l'absence de réponse à une communication. Le consentement doit couvrir toutes les activités de traitement effectuées pour la même finalité. Lorsque le traitement a des finalités multiples, un consentement spécifique doit être donné pour chacune de ces finalités.

Lorsque le Groupe Proximus fournit des services de la société de l'information (c'est-à-dire des services en ligne) directement aux enfants, il s'assurera d'avoir obtenu le consentement du titulaire de la responsabilité parentale à l'égard de l'enfant lors du traitement des données personnelles.

Proximus doit être en mesure de démontrer, pour chaque personne concernée, qu'un consentement valable a été obtenu pour toutes les activités de traitement des données personnelles pour lesquelles la base juridique appropriée est le consentement.

2.7 Catégories particulières de données personnelles

Le traitement de catégories particulières de données personnelles[11], telles que les données personnelles révélant l'origine ethnique, les convictions religieuses, l'appartenance syndicale ou les données concernant la santé[12], et le traitement des données judiciaires[13] sont en principe interdits, sauf dans des circonstances spécifiques, par exemple si la personne concernée a donné son consentement explicite pour un tel traitement.

Les conditions juridiques spécifiques au traitement des catégories particulières de données personnelles et des données judiciaires sont analysées et documentées dans le cadre de la procédure de « privacy by design ».

2.8 Violations de données personnelles

2.8.1 Général

Le Groupe Proximus doit maintenir et mettre en œuvre une procédure appropriée pour gérer les violations de données personnelles[14]. L'autorité de contrôle doit être notifiée lorsqu'une violation de données personnelles est connue et qu'elle est susceptible d'entraîner un risque pour les droits et libertés des personnes physiques. Dans ce cas, l'autorité de contrôle doit être informée dans les meilleurs délais et, si possible, au plus tard 72 heures après avoir pris connaissance de la violation des données personnelles.

En outre, lorsqu'une violation de données personnelles est susceptible d'entraîner un risque élevé pour les droits et libertés des personnes physiques, le Groupe Proximus doit communiquer la violation des données personnelles aux personnes concernées dans les meilleurs délais.

De plus, conformément à la Directive e-Privacy, le Groupe Proximus est tenu de notifier à l'autorité de contrôle toute violation de données à caractère personnel en rapport avec la fourniture d'un service de communications électroniques accessible au public, dans la mesure du possible 24 heures au plus tard après la détection de la violation des données personnelles. La détection de données à caractère personnel est supposée avoir lieu lorsque le Groupe Proximus a suffisamment pris conscience qu'un incident de sécurité compromettant des données personnelles s'est produit, pour effectuer une notification pertinente.

Lorsque la violation des données personnelles est susceptible de porter atteinte aux données personnelles ou à la vie privée d'un abonné ou d'une personne, le Groupe Proximus devra également informer l'abonné ou la personne dans les meilleurs délais de la violation des données personnelles.

[11] Voir la définition de « catégories particulières de données personnelles » à l'Annexe 1.
[12] Voir la définition de « données concernant la santé » à l'Annexe 1.
[13] Voir la définition de « données judiciaires » à l'Annexe 1.
[14] Voir la définition de « violation de données personnelles » à l'Annexe 1.

2.8.2 Améliorations continues

Conformément à sa stratégie « Bold 2025 », Proximus s'engage à préserver la confidentialité et la sécurité des données personnelles qu'elle traite. Pour respecter cet engagement, Proximus reconnaît l'importance d'une amélioration continue de ses mesures de protection des données et s'engage à établir des priorités et à mettre en œuvre rapidement les améliorations structurelles nécessaires pour réduire le risque de violation des données, d'accès non autorisé, etc.

En outre, Proximus est consciente que le paysage de la protection des données est en constante évolution et que de nouveaux défis peuvent se présenter. Dans le cadre de la présente politique, Proximus s'engage à se tenir au courant des dernières normes industrielles, des meilleures pratiques et des exigences légales afin de s'assurer que ses mesures de protection des données restent à la pointe de la protection.

En édictant et en adhérant à ces principes, Proximus démontre son engagement ferme à protéger les données personnelles qu'elle traite. Grâce à des efforts continus pour prioriser et mettre en œuvre des améliorations structurelles, Proximus vise à protéger les données personnelles et à maintenir le plus haut niveau de protection des données, renforçant ainsi la confiance dans sa marque.

2.9 Partage de données personnelles

Le Groupe Proximus doit veiller à ce que les données personnelles ne soient pas communiquées à des tiers non autorisés, que ce soit en interne (c'est-à-dire au sein du Groupe Proximus) ou en externe (c'est-à-dire en dehors du Groupe Proximus). Tous les employés doivent faire preuve de prudence lorsqu'il leur est demandé de partager avec un tiers des données personnelles concernant un autre individu. Il est important de se demander si la divulgation des données personnelles est pertinente et nécessaire à la réalisation des activités du Groupe Proximus.

Le partage de données personnelles constitue un traitement de données personnelles qui est soumis à tous les principes énumérés dans la section 2.2 de la présente politique. En particulier, le principe de licéité du RGPD exige qu'il y ait une base juridique[15] pour le partage des données personnelles, et que cette base juridique soit documentée. Le partage des données personnelles doit toujours faire l'objet de mesures de sécurité appropriées[16]. La licéité et les autres obligations légales applicables au partage des données personnelles doivent être analysées et documentées dans le cadre de la procédure de « privacy by design ».

2.9.1 Échanges de données au sein du Groupe Proximus

L'échange de données personnelles entre les entités du Groupe Proximus n'est exempt d'aucune restriction et doit respecter toutes les conditions relatives au partage de données personnelles expliquées dans cette section 2.9.

[15] Le principe de licéité est expliqué à la section 2.2.1.1.
[16] Le principe de sécurité des données personnelles est expliqué à la section 2.2.6.

Il convient par ailleurs de tenir compte des restrictions imposées par la loi sur la concurrence (voir la politique « Concurrence incl. Chinese Walls, Echanges d'Information et Dawn Raids »).

2.9.2 Transfert de données à caractère personnel en dehors de l'UE

Le Groupe Proximus s'engage à mettre en place des mesures de protection adéquates, conformément à la législation en vigueur, pour protéger les données personnelles transférées par le Groupe Proximus vers des pays qui ne disposent pas d'une législation adéquate en matière de protection des données.

Lors du transfert de données personnelles vers un pays non-membre de l'Espace économique européen (**pays tiers**), l'un des outils suivants, conformément au chapitre V du RGPD, doit être utilisé pour garantir le niveau adéquat de protection des données :

- La reconnaissance, par une décision de la Commission européenne (**décision d'adéquation**), d'un régime de protection des données adéquat dans le pays où se trouve le destinataire des données personnelles.
- En l'absence d'une décision d'adéquation, un transfert peut avoir lieu moyennant la mise en place de garanties appropriées.
  Les accords contractuels avec le destinataire des données personnelles, en utilisant par exemple les clauses contractuelles types approuvées par la Commission européenne, sont un exemple de ces garanties appropriées.
- Enfin, si un transfert de données personnelles est envisagé vers un pays tiers qui ne fait pas l'objet d'une décision d'adéquation et s'il n'existe pas de garantie appropriée, un transfert peut être effectué sur la base d'un certain nombre de dérogations pour des situations spécifiques ; par exemple, lorsqu'une personne a explicitement consenti au transfert proposé après avoir reçu toutes les informations nécessaires sur les risques associés au transfert.

2.9.3 Sous-traitants

Le Groupe Proximus identifie pour chaque produit/service standard le rôle de l'entité concernée par rapport au traitement des données personnelles (c.-à-d. responsable du traitement, sous-traitant[17]) et veille à ce que les clauses contractuelles correctes soient stipulées dans le contrat, reflétant les responsabilités et obligations adéquates liées à ce rôle.

Dans le cas où une entité du Groupe Proximus ou l'autre partie fournissant des services au Groupe Proximus agit en tant que sous-traitant, le contrat conclu par les parties doit spécifier les devoirs du sous-traitant envers le responsable du traitement conformément à l'article 28 du RGPD (**contrat de traitement des données**).

[17] Voir les définitions de « responsable du traitement » et de « sous-traitant » à l'Annexe 1.

2.9.4 Responsables conjoints

Si une entité du Groupe Proximus traite des données personnelles en tant que responsable conjoint du traitement[18] avec une ou plusieurs organisations, elle doit conclure avec cette ou ces organisations un accord définissant leurs responsabilités respectives en matière de respect des obligations prévues par le RGPD. Les principaux aspects de cet accord doivent être communiqués aux personnes concernées.

2.10 Sensibilisation et formation

Le Groupe Proximus encourage les programmes de formation et de sensibilisation et met à disposition des ressources afin de sensibiliser et de fournir des formations générales et spécifiques sur la protection des données, sur les aspects pertinents pour les rôles et responsabilités de chacun. Les employés de Proximus doivent suivre et achever toutes les formations requises en matière de protection des données et de sécurité de l'information.

2.11 Registre des activités de traitement

Conformément à l'article 30 du RGPD et afin de s'assurer que le Groupe Proximus comprenne les données personnelles qu'il traite, les finalités pour lesquelles il les traite et le niveau de risque lié au traitement de ces données, le Groupe Proximus tient un registre des activités de traitement dans lequel sont documentées toutes les activités de traitement des données personnelles gérées sous la responsabilité de Proximus, en tant que responsable du traitement, responsable conjoint du traitement et sous-traitant.

3. Politique: Secret des communications électroniques

3.1 Principe

Le secret des communications électroniques protège le contenu des appels et les données de communications électroniques comme les numéros appelés, la durée de la communication, la connexion internet, et la confidentialité des numéros privés (**données de communications électroniques**[19]). Il y a lieu de traiter en toute confidentialité aussi bien le contenu d'une communication que les données s'y rapportant (métadonnées).

Protection du contenu de la communication

[18] Voir la définition de « responsable conjoint du traitement » à l'Annexe 1.
[19] Voir la définition de « données de communications électroniques » à l'Annexe 1.

Une personne qui ne participe pas à une communication (communication mobile, fixe ou de données) n'a pas le droit d'essayer de découvrir le contenu de la communication transmise. Il est également interdit d'enregistrer le contenu de communications.

Protection des données relatives à une communication (métadonnées)

Il est interdit de découvrir, divulguer, modifier ou détruire intentionnellement des données relatives à des communications électroniques concernant d'autres personnes ou d'identifier les personnes concernées.

3.2 Exceptions

La loi définit un certain nombre de situations dans lesquelles cette interdiction ne s'applique pas à un opérateur télécom et ses employés (voir liste non-exhaustive ci-dessous).

Veuillez contacter le conseiller compétent du département juridique pour examiner si une exception peut être appliquée. Exemple d'exceptions :

- Il est nécessaire de vérifier le réseau pour s'assurer qu'il fonctionne correctement ou que le service de télécommunications est fourni correctement ;
- Toutes les parties participant à la communication ont donné leur consentement ;
- Les métadonnées relatives aux communications électroniques (pas le contenu de la communication) sont utilisées aux fins spécifiques suivantes :
    - facturation et paiements d'interconnexion ;
    - marketing direct avec le consentement du client ;
    - suivi des offres et services de données de trafic ;
    - gestion de trafic ;
    - détection de fraudes.

La réglementation prévoit également des exceptions à la confidentialité des télécommunications pour les autorités judiciaires, les services d'urgence, l'Institut Belge des Services Postaux et des Télécommunications, le service de médiation pour les télécommunications.

Des exceptions prévues par la loi permettent par ailleurs l'enregistrement d'une communication à des fins de contrôle de la qualité dans les call centers et en tant que preuve de transactions commerciales.

3.3 Amendes et sanctions

Toute violation de la Directive e-Privacy peut faire l'objet d'amendes allant jusqu'à 800.000€ et de peines de prison allant jusqu'à 4 ans.

4. Surveillance et contrôle

Afin de contrôler le respect par le Groupe Proximus de la législation en matière de protection des données, le Groupe Proximus doit :

- maintenir un cadre définissant les contrôles internes appropriés et les mécanismes de supervision indépendants pour contrôler le respect des lois pertinentes et des politiques et procédures en matière de protection des données ;

- développer, maintenir et appliquer une procédure de « privacy by design » afin d'analyser si les nouveaux produits/services impliquant le traitement de données personnelles sont conformes aux obligations en matière de protection des données ;
- effectuer des contrôles de conformité ad hoc effectués par le Data Protection Office ;
- réaliser des audits ad hoc par des auditeurs internes ou des auditeurs externes de confiance.

Annexe 1 : Définitions

Autorité de contrôle (Autorité de protection des données) - une autorité publique indépendante qui est instituée par un État membre. En Belgique, l'autorité de contrôle est l' « Autorité de protection des données ».

Catégories particulières de données personnelles - données personnelles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que les données génétiques, les données biométriques aux fins d'identifier une personne physique de manière unique, les données concernant la santé ou les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

Consentement de la personne concernée - toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données personnelles la concernant fassent l'objet d'un traitement.

Directive e-Privacy (directive vie privée et communications électroniques) - la Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et assure la protection des libertés et droits fondamentaux, notamment le respect de la vie privée, la confidentialité des communications et la protection des données personnelles dans le secteur des communications électroniques. La Directive a été transposée en droit belge par la loi du 13 juin 2005 relative aux communications électroniques.

Données biométriques - données personnelles résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques.

Données concernant la santé - les données personnelles relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne.

Données de communications électroniques - données relatives au trafic et données de localisation. Les données relatives au trafic désignent toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation. Les données de localisation désignent toutes les données traitées dans un réseau de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public.

Données génétiques - les données personnelles relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question.

Données judiciaires - données personnelles relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes.

Données personnelles – ou « données à caractère personnel » - toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des

données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Enfant - le RGPD définit un enfant comme toute personne âgée de moins de 16 ans. Le traitement des données personnelles d'un enfant de moins de 13 ans n'est licite que si le consentement des parents ou du tuteur a été obtenu.

Établissement - l'établissement principal du responsable du traitement dans l'UE est le lieu où il prend les principales décisions quant à la finalité de ses activités de traitement des données. L'établissement principal d'un sous-traitant dans l'UE sera son centre administratif. Si un responsable du traitement est établi en dehors de l'UE, il devra désigner un représentant dans la juridiction dans laquelle il opère, pour agir au nom du responsable du traitement et traiter avec les autorités de contrôle.

Personne concernée - toute personne physique vivante qui est le sujet de données personnelles détenues par une organisation.

Profilage - toute forme de traitement automatisé de données personnelles consistant à utiliser ces données personnelles pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique.

Responsable conjoint du traitement - un responsable du traitement qui détermine les finalités et les moyens du traitement des données personnelles conjointement avec un ou plusieurs autres responsables du traitement.

Responsable du traitement - la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre.

RGPD (Règlement général sur la protection des données) – 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, et abrogeant la directive 95/46/CE.

Sous-traitant - la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données personnelles pour le compte du responsable du traitement.

Tiers - une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données personnelles.

Traitement - toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données personnelles, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

Violation de données personnelles - une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données personnelles transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.