proximus

DPO

Bescherming van persoonsgegevens en elektronisch communicatiegeheim

Last update on 17/12/2024
Owner Data Protection Officer

Inhoudsopgave

1. Inleiding

1.1 Doel van de policy

De Proximus Group heeft zich ertoe verbonden alle toepasselijke wetten inzake bescherming van persoonsgegevens en alle goede praktijken met betrekking tot de verwerking van gegevens inzake elektronische communicatie en persoonsgegevens, zoals bepaald in deze policy, na te leven.

Het is belangrijk om elektronische communicatiegegevens en persoonsgegevens strikt vertrouwelijk te behandelen omdat deze gegevens wettelijk beschermd zijn. Indien een entiteit van de Proximus Group of een of meer van zijn werknemers, contractanten of vertegenwoordigers nalaat om zich naar deze wettelijke verplichtingen te schikken, kan dit aanleiding geven tot strafrechtelijke, administratieve en disciplinaire sancties

Het spreekt voor zich dat het in acht nemen van het elektronisch communicatiegeheim en de privacy van onze klanten vooropstaat als we klanten en hun vertrouwen willen winnen en behouden.

De Proximus Group heeft zich ertoe verbonden alle toepasselijke wetgeving i.v.m. persoonsgegevens na te leven, en de rechten en vrijheden van individuele personen te beschermen in overeenstemming met o.m. de Algemene Verordening Gegevensbescherming (**AVG**[1]) en de Richtlijn betreffende privacy en elektronische communicatie (**e-Privacyrichtlijn**[2]), omgezet in de Belgische wetgeving via de wet betreffende de elektronische communicatie van 13/06/2005.

1.2 Toepassingsgebied van de policy

Deze policy is van toepassing op alle medewerkers en (sub)contractanten van de Proximus Group en op alle verwerkingen van persoonsgegevens[3], met inbegrip van gegevens inzake elektronische communicatie[4], door de Proximus Group, hetzij als verwerkingsverantwoordelijke, hetzij als verwerker van deze gegevens[5]. Dit omvat de persoonsgegevens van elk van de volgende categorieën van betrokkenen[6]: actieve Proximus-klanten, potentiële klanten en vroegere klanten, sollicitanten, huidige Proximus-medewerkers en - (sub)contractanten en vroegere Proximus-medewerkers en -(sub)contractanten.

[1] Zie definitie van "AVG" in Bijlage 1.
[2] Zie definitie van "e-Privacyrichtlijn" in Bijlage 1.
[3] Zie definitie van "persoonsgegevens" in Bijlage 1.
[4] Zie definitie van "gegevens inzake elektronische communicatie" in Bijlage 1.
[5] Zie definitie van "verwerkingsverantwoordelijke" en "verwerker" in Bijlage 1.
[6] Zie definitie van "betrokkene" in Bijlage 1.

In deze policy verwijst de term “Proximus Group” naar Proximus NV, een naamloze vennootschap onder Belgisch publiek recht (**Proximus**), en haar dochtervennootschappen. Dochtervennootschappen kunnen waar nodig deze policy aanpassen of ervan afwijken om te voldoen aan specifieke lokale wettelijke vereisten die afwijken van deze policy, zodat de naleving van de toepasselijke lokale wetgeving wordt verzekerd.

Medewerkers en (sub)contractanten van de Proximus Group en elke derde partij die werkt met of voor de Proximus Group en die toegang (zouden kunnen) hebben, worden verwacht deze policy te lezen, te begrijpen en overeenkomstig de policy te handelen. Merk op dat in het vervolg van dit beleid de term "Proximus-medewerker" zowel werknemers als (onder)aannemers van de Proximus Groep omvat.

Deze policy is in lijn met de AVG en met de e-Privacyrichtlijn.

De AVG is van toepassing op alle verwerkingsverantwoordelijken die gevestigd zijn in de Europese Unie (**EU**) en persoonsgegevens van betrokkenen verwerken, in het kader van de activiteiten van die vestiging[7]. De AVG is ook van toepassing op verwerkingsverantwoordelijken die gevestigd zijn buiten de EU en persoonsgegevens verwerken van betrokkenen die zich in de EU bevinden en de verwerkingsactiviteiten gelinkt zijn aan:

- de aanbieding van goederen en diensten aan deze betrokkenen in de EU, ongeacht of een betaling door de betrokkenen is vereist; of
- het monitoren van hun gedrag, voor zover dit gedrag in de EU plaatsvindt.

1.3 Wat moeten Proximus-medewerkers doen?

Dit deel heeft tot doel een overzicht te geven van de actiepunten die Proximus-medewerkers moeten opnemen om aan de vereisten van deze policy te voldoen. Onderstaande lijst is niet-exhaustief en heeft enkel tot doel de belangrijkste vereisten op een hands-on manier in de verf te zetten.

1.3.1 De principes van verwerking van persoonsgegevens toepassen wanneer persoonsgegevens worden verzameld en gebruikt

- Alleen persoonsgegevens verzamelen die rechtstreeks relevant en noodzakelijk zijn voor het bereiken van het/de gespecificeerde doel(en) en persoonsgegevens alleen bewaren zolang dat nodig is om het/de gespecificeerde doel(en) te bereiken.
- Persoonsgegevens alleen gebruiken voor het doel of de doelen waarvoor ze zijn verzameld.
- Ervoor zorgen dat persoonsgegevens correct en up-to-date zijn en relevant zijn voor het doel of de doelen waarvoor zij worden verzameld.
- Persoonsgegevens (op papier en elektronisch) beveiligen door middel van passende beveiligingsmaatregelen tegen risico's zoals verlies, ongeoorloofde toegang of gebruik, vernietiging, wijziging of onbedoelde of ongepaste openbaarmaking.

[7] Zie definitie van “vestiging” in Bijlage 1.

- Geen toegang hebben tot persoonsgegevens en geen persoonsgegevens verzamelen of opslaan die niet noodzakelijk zijn voor hun huidige takenpakket.
- Persoonsgegevens altijd veilig verwijderen wanneer ze niet langer nodig zijn voor het/de gespecificeerde doel(en).

1.3.2 Het privacy by design-proces volgen

- Het privacy by design-proces[8] volgen tijdens de eerste ontwerpfase van elk systeem, product of proces waarbij persoonsgegevens worden verwerkt.
- De maatregelen die gedefinieerd werden in het kader van het privacy by design-proces implementeren teneinde de risico's die deze verwerkingsactiviteit kan inhouden voor de rechten en de vrijheden van de betrokkenen te beperken.

1.3.3 Inbreuken in verband met persoonsgegevens en klachten melden

- Elke vermoedelijke inbreuk in verband met persoonsgegevens overeenkomstig de interne meldingsprocedures melden. Een inbreuk in verband met persoonsgegevens doet zich voor wanneer de vertrouwelijkheid, beschikbaarheid of integriteit van persoonsgegevens in het gedrang komt.
- Klachten van betrokkenen over de verwerking van hun persoonsgegevens overeenkomstig de interne meldingsprocedures melden.

1.3.4 Vereiste opleidingen voltooien

- Alle vereiste opleidingen op het gebied van bescherming van persoonsgegevens en informatiebeveiliging volgen en voltooien.

1.4 Verantwoordelijkheden

Dit deel identificeert en licht de taken en verantwoordelijkheden van de verschillende actoren die betrokken zijn bij de naleving van de wetgeving inzake bescherming van persoonsgegevens toe. Deze rollen zijn op een algemene manier gedefinieerd zodat ze toepasbaar zijn in alle dochtervennootschappen van de Proximus Group, rekening houdend met hun respectievelijke behoeften en bedrijfsstructuur.

[8] Het privacy by design-proces is een process dat werd opgezet om bij het ontwerp van elk initiatief waarbij persoonsgegevens worden verwerkt, rekening te houden met de vereisten inzake bescherming van persoonsgegevens. Zie sectie 2.3.

1.4.1 Proximus Group

Proximus of een van haar dochterondernemingen kunnen zowel als verwerkingsverantwoordelijke als als verwerker[9] gekwalificeerd worden onder de AVG. Proximus of haar dochteronderneming zijn in hun rol van verwerkingsverantwoordelijke /verwerker verantwoordelijk voor de naleving van de AVG en moet kunnen aantonen dat er wordt gehandeld in overeenstemming met de AVG (verantwoordingsplicht)[10].

Het senior management en al wie bij Proximus een managementfunctie of toezichthoudende functie uitoefent, is verantwoordelijk voor het ontwikkelen en bevorderen van goede praktijken inzake bescherming van persoonsgegevens.

1.4.2 Alle medewerkers

De wetgeving inzake de bescherming van persoonsgegevens naleven is de verantwoordelijkheid van alle Proximus-medewerkers, zowel de werknemers als de (onder)aannemers van de Proximus Group, die persoonsgegevens verwerken.

Sectie 1.3 biedt een niet-exhaustief overzicht van de actiepunten die alle Proximus-medewerkers moeten volgen teneinde de voorschriften van dit beleid na te volgen.

1.4.3 Data Protection Officer

Indien wettelijk vereist, wordt een Data Protection Officer ("DPO") aangesteld om toe te zien op de verwerking van persoonsgegevens door een of meer dochtervennootschappen van de Proximus Group. De verantwoordelijkheden van de DPO omvatten onder meer:

- Toezien op de naleving van de AVG en andere toepasselijke wetgeving inzake bescherming van persoonsgegevens, alsook op de Proximus policies (met inbegrip van deze policy);
- De medewerkers en het management van Proximus informeren en adviseren over de verplichtingen inzake bescherming van persoonsgegevens;
- Rapporteren over vereisten, risico's en gevolgen in verband met bescherming van persoonsgegevens en privacy aan het management;
- Samenwerken met de toezichthoudende autoriteiten en optreden als aanspreekpunt voor toezichthoudende autoriteiten en betrokkenen in dossiers omtrent bescherming van persoonsgegevens;
- Erop toezien dat gegevensbeschermingseffectbeoordelingen of 'data protection impact assessments' in het Engels ("DPIA") worden uitgevoerd voor verwerkingsactiviteiten met een hoog risico en – waar nodig – adviseren tijdens het DPIA-proces;

[9] Zie definitie van "verwerkingsverantwoordelijke" en "verwerker" in Bijlage 1.
[10] Het principe van de verantwoordingsplicht wordt uitgelegd in sectie 2.2.7.

- Algemene training voorzien en bewustwording creëren om ervoor te zorgen dat de hele organisatie de AVG en andere toepasselijke wetgeving inzake bescherming van persoonsgegevens begrijpt en naleeft.

1.4.4 Ondersteunende teams

Afhankelijk van de behoeften van de betrokken dochtervennootschap van de Proximus Group, bieden verschillende ondersteunende teams gespecialiseerde expertise aan om de naleving van de vereisten inzake bescherming van persoonsgegevens te implementeren en te handhaven, waaronder:

- **Experts inzake informatiebeveiliging**: ervoor zorgen dat de technische en organisatorische maatregelen aanwezig zijn om persoonsgegevens te beschermen tegen ongeautoriseerde toegang, inbreuken en gegevensverlies en het beheren van cyberbeveiligingsincidenten.
- **Juridische experts**: adviseren over de interpretatie van de vereisten inzake bescherming van persoonsgegevens en toezien op de naleving van de toepasselijke wetgeving in contracten en operationele handelingen.
- **Experts inzake gegevensbeheer** (‘**data governance**’ in het Engels): ondersteuning bij het bijhouden van gegevensinventarissen en het waarborgen van een goed beheer van de levenscyclus van gegevens.
- **Auditteams**: de naleving van het policies inzake bescherming van persoonsgegevens controleren en evalueren.

1.4.5 Bestuursorganen

Specifieke bestuursorganen samengesteld uit leden van het management die verantwoordelijk zijn voor het toezicht op en het nemen van beslissingen omtrent risico's met betrekking tot bescherming van persoonsgegevens en de naleving van de AVG.

2. Policy: Bescherming van persoonsgegevens

2.1 Gevolgen in geval van niet-naleving

2.1.1 AVG

De AVG trad in werking op 25 mei 2018 en bevatte geen overgangsbepalingen voor bestaande persoonsgegevens. Dit betekent dat de Proximus Group vanaf die datum volledig moet voldoen aan de AVG.

De Proximus Group stelt zowel verwerkingsactiviteiten in de hoedanigheid van verwerkingsverantwoordelijke als in de hoedanigheid van verwerker en riskeert sancties in geval van niet-naleving van zijn verplichtingen onder de wetgeving inzake bescherming van persoonsgegevens.

De AVG voorziet in verschillende soorten sancties in geval van niet-naleving van de regels inzake bescherming van persoonsgegevens, waaronder berispingen, een tijdelijk of definitief verwerkingsverbod

en boetes van maximaal 20 miljoen euro of 4% van de totale wereldwijde jaaromzet in het voorgaande boekjaar.

2.1.2 Wet betreffende de elektronische communicatie van 13/06/2005

Mogelijke sancties in geval van niet-naleving van de e-Privacyrichtlijn werden opgenomen in sectie 3.3.

2.1.3 Tuchtsancties

Elke schending van dit beleid kan aanleiding geven tot disciplinaire maatregelen die kunnen leiden tot ontslag, in overeenstemming met de toepasselijke arbeidswetgeving. Inbreuken op de wetgeving inzake bescherming van persoonsgegevens kunnen ook een strafbaar feit uitmaken. In dat geval wordt de zaak zo snel mogelijk gemeld aan de bevoegde autoriteiten.

2.2 Principes m.b.t. de verwerking van de persoonsgegevens

Elke verwerking van persoonsgegevens dient te gebeuren in overeenstemming met de volgende principes inzake bescherming van persoonsgegevens. Alle nieuwe producten en diensten waarbij persoonsgegevens worden verwerkt, moeten het privacy by design-proces volgen om ervoor te zorgen dat van bij het initiële ontwerp rekening wordt gehouden met deze principes.

2.2.1 Rechtmatigheid, behoorlijkheid en transparantie

Persoonsgegevens moeten rechtmatig, behoorlijk en transparant verwerkt worden.

2.2.1.1 Rechtmatigheid

De verwerking van de persoonsgegevens dient op rechtmatige wijze te gebeuren. Opdat de verwerking als rechtmatig wordt beschouwd, dient ze op een van de rechtsgronden, opgesomd in artikel 6.1 AVG, te steunen, namelijk:

- Voorafgaande toestemming van de betrokkene;
- Uitvoering van een contract;
- Naleving van een wettelijke verplichting in hoofde van de verwerkingsverantwoordelijke;
- Bescherming van de vitale belangen van de betrokkene;
- Uitoefening van het openbare belang of van het openbare gezag; of
- Gerechtvaardigd belang van Proximus of een derde.

Er bestaat geen hiërarchie tussen deze verschillende rechtsgronden.

De verwerkingsactiviteit waarbij bijzondere categorieën van persoonsgegevens verwerkt worden, dient te steunen op een specifieke rechtsgrond[11].

Meer in het algemeen betekent rechtmatigheid ook dat de verwerking van persoonsgegevens niet onwettig of illegaal mag zijn. Dit houdt in dat alle verwerkingsactiviteiten in overeenstemming moeten zijn met de toepasselijke strafrechtelijke en civielrechtelijke wetten en beginselen.

In het privacy by design-proces, dat gevolg moet worden voor elk niet initiatief waarin persoonsgegevens worden verwerkt, wordt de geschikte rechtsgrond voor de verwerkingsactiviteit bepaald en gedocumenteerd.

2.2.1.2 Behoorlijkheid

De persoonsgegevens moeten op behoorlijke wijze worden verwerkt. Dit houdt in dat:

- De Proximus Group de persoonsgegevens verwerkt op een manier die de betrokkenen redelijkerwijze verwachten (transparantie en redelijke verwachtingen);
- De Proximus Group de persoonsgegevens niet gebruikt op een manier die een nadelige impact heeft op de betrokkene;
- De Proximus Group de betrokkenen niet misleidt;
- De Proximus Group de betrokkenen niet misleidt om hun persoonsgegevens te laten verwerken.

2.2.1.3 Transparantie

De vereisten m.b.t. de informatie die aan de betrokkenen moet worden beschikbaar gesteld, werd uitgebreid in de AVG. Het transparantiebeginsel bepaalt welke informatie i.v.m. de verwerking van persoonsgegevens aan de betrokkenen moet worden gegeven, alsook het tijdstip en de wijze waarop die informatie verstrekt moet worden.

De verplichte inhoud van de informatie die aan de betrokkenen moet worden meegedeeld is vastgelegd in de artikelen 13.1 en 13.2 or 14.1 en 14.2 van de AVG.

Informatie en communicatie in verband met de verwerking van persoonsgegevens moet:

- beknopt, transparant, begrijpelijk en gemakkelijk toegankelijk zijn;
- in duidelijke en eenvoudige taal opgesteld zijn;
- schriftelijk of met andere middelen, met inbegrip van, indien dit passend is, elektronische middelen verstrekt worden; en
- gratis zijn.

De informatie met betrekking tot de verwerking van persoonsgegevens moet aan de betrokkenen worden verstrekt binnen de in artikel 13.1, en artikel 14.3, onder a) tot en met c), van de AVG vastgestelde termijnen.

[11] Zie definitie van "bijzondere categorieën van persoonsgegevens" in Bijlage 1.

2.2.2 Doelbinding

Persoonsgegevens mogen alleen worden verzameld en verwerkt voor specifieke, legitieme en expliciete doeleinden en mogen niet verder worden verwerkt op een manier die niet compatibel is met deze doeleinden. In het privacy by design-proces wordt gecontroleerd en gedocumenteerd of een verwerking van persoonsgegevens wordt gerechtvaardigd door een geldig doel of dat een nieuw doel verenigbaar is met het oorspronkelijke doel van de verwerking.

2.2.2.1 Specifiek doel

Het doel van de verwerking van persoonsgegevens moet vooraf worden vastgesteld en moet worden bepaald op het tijdstip waarop de persoonsgegevens worden verzameld of verder worden verwerkt.

Indien de verwerkingsactiviteit geen specifiek doel dient, mag ze niet plaatsvinden. De verwerkingsactiviteit moet onmiddellijk worden stopgezet wanneer het doel van de verwerking niet langer bestaat.

2.2.2.2 Legitiem doel

Een doel is legitiem wanneer het in overeenstemming is met alle wettelijke vereisten en wanneer het rechtsgeldig is. Daarnaast moet een doel ook redelijk en realistisch zijn om aangemerkt te worden als een legitiem doel.

2.2.2.3 Uitdrukkelijk doel

Een doel is uitdrukkelijk wanneer het duidelijk wordt bekendgemaakt, uitgelegd en uitgedrukt, en dit uiterlijk op het ogenblik dat de persoonsgegevens worden verzameld of verder worden verwerkt.

2.2.2.4 Compatibel gebruik

Persoonsgegevens die worden verkregen voor specifieke doeleinden mogen achteraf niet worden gebruikt voor andere doeleinden die niet compatibel zijn met het doel dat initieel was vastgelegd. Niettemin kunnen persoonsgegevens voor een nieuw doel verwerkt worden wanneer de persoonsgegevens zijn verzameld op grond van een overeenkomst of op grond van een gerechtvaardigd of een vitaal belang, maar slechts nadat werd nagegaan of het nieuwe doel verenigbaar is met het oorspronkelijke doel.

2.2.3 Minimale gegevensverwerking

De persoonsgegevens moeten toereikend (voldoende om het vooropgestelde doel te bereiken), ter zake dienend (met een rationele link naar het doel) en beperkt zijn tot wat noodzakelijk is met betrekking tot de doeleinden waarvoor ze verwerkt worden.

Indien bepaalde persoonsgegevens niet strikt noodzakelijk zijn voor de vooropgestelde doeleinden, mogen deze persoonsgegevens niet verzameld of verwerkt worden.

De methoden voor het verzamelen van persoonsgegevens worden herzien in het kader van het privacy by design-proces om ervoor te zorgen dat de verzamelde gegevens nog steeds toereikend, ter zake dienend en niet buitensporig zijn.

2.2.4 Juistheid

Persoonsgegevens moeten juist zijn en up-to-date worden gehouden.

Om de juistheid te verzekeren, moeten persoonsgegevens zoveel mogelijk van de betrokkenen zelf worden verkregen. Persoonsgegevens die voor lange tijd worden bijgehouden door de Proximus Group, moeten worden gereviewd en bijgewerkt waar nodig.

2.2.5 Opslagbeperking

Persoonsgegevens mogen in een zodanige vorm worden bewaard dat de betrokkene niet langer kan worden geïdentificeerd dan noodzakelijk is voor de verwezenlijking van de doeleinden waarvoor zij worden verwerkt. Persoonsgegevens mogen niet voor onbepaalde tijd worden bewaard. De duur van de periode kan variëren afhankelijk van het doel waarvoor de persoonsgegevens worden verwerkt. Gedurende de gehele periode moet Proximus Group kunnen aantonen dat de opslag van de persoonsgegevens noodzakelijk is voor dat doel.

De passende bewaartermijn van de persoonsgegevens wordt gedefinieerd en gedocumenteerd als onderdeel van het privacy by design-proces dat moet worden gevolgd voor elk nieuw initiatief waarbij persoonsgegevens worden verwerkt.

De Proximus Groep moet ervoor zorgen dat de persoonsgegevens aan het einde van de bewaartermijn veilig worden geanonimiseerd, verwijderd of vernietigd.

2.2.6 Beveiliging van persoonsgegevens

Persoonsgegevens moeten worden verwerkt op een manier die een passende beveiliging van de persoonsgegevens waarborgt, met inbegrip van bescherming tegen ongeoorloofde of onwettige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging, aan de hand van passende technische of organisatorische maatregelen. De Proximus Group zal zulke technische en organisatorische maatregelen treffen om een passende beveiliging van de persoonsgegevens te waarborgen.

Alle persoonsgegevens worden geclassificeerd en behandeld in functie van hun gevoeligheidsniveau zoals bepaald in het Proximusbeleid inzake informatie-eigendom en -classificatie.

Bij de beoordeling van de maatregelen om een passend beveiligingsniveau van persoonsgegevens te waarborgen, zal een risicobeoordeling uitgevoerd worden waarbij rekening wordt gehouden met alle omstandigheden van de verwerkingsactiviteiten van de Proximus Group, alsmede met de omvang van de mogelijke schade of het mogelijke verlies dat aan de betrokkenen kan worden berokkend indien zich een inbreuk op de beveiliging voordoet, de gevolgen van een eventuele inbreuk op de beveiliging voor de Proximus Group zelf, en mogelijke reputatieschade, met inbegrip van een mogelijk verlies van vertrouwen bij de klant.

Bij het evalueren van de gepaste technische maatregelen zullen onder meer de volgende maatregelen worden overwogen:

- Firewalls en internetgateways;
- Privacyverhogende technieken zoals pseudonimisering en anonimisering;
- Identiteits- en toegangsbeheer (waaronder Public Key Infrastructure, Key Management Infrastructure, enz.);
- Beheer van bedreigingen en kwetsbaarheden (waaronder scanning en patching van kwetsbaarheden, loggen en monitoren van events, bescherming tegen malware en inbraakdetectie);
- Preventie tegen datalekken;
- Versleutelingsbeheer;
- Beveiliging van applicaties (waaronder SOA-beveiliging, databasebeveiliging);
- Bescherming van netwerkcomponenten en toestellen van eindgebruikers;
- Security Information en Event Management;
- Scheiding van data, applicaties en netwerken;
- Audit logs en monitoring;
- Beheer van de toegang op afstand van leveranciers en derden.

Bij het evalueren van de gepaste organisatorische maatregelen zullen onder meer de volgende maatregelen worden overwogen:

- Kader voor beleidslijnen inzake bescherming van persoonsgegevens;
- Opleiden en sensibiliseren van Proximus-medewerkers;
- Fysieke toegangscontroles;
- 'Clear desk policy' implementeren.

Alle Proximus-medewerkers dienen erover te waken dat alle persoonsgegevens die de Proximus Group in bezit heeft en waarvoor ze verantwoordelijk zijn, veilig worden bijgehouden.

2.2.6.1 Integriteit

Persoonsgegevens moeten naar behoren worden beveiligd om hun integriteit te verwezenlijken en te behouden. Tijdens de gehele levenscyclus van een project of proces moet rekening worden gehouden met de integriteit van de gegevens.

2.2.6.2 Vertrouwelijkheid

Volgens het need to know-princpe mogen persoonsgegevens niet toegankelijk zijn voor personen die ze niet nodig hebben. De toegang tot persoonsgegevens moet altijd beperkt blijven tot de personen die ze nodig hebben voor de uitvoering van hun taken. De Proximus Group moet ervoor zorgen dat persoonsgegevens alleen worden verwerkt door bevoegde medewerkers of apparatuur.

2.2.7 Verantwoordingsplicht

Krachtens artikel 5.2 van de AVG is de Proximus Group als verwerkingsverantwoordelijke niet alleen verantwoordelijk voor de naleving van de AVG, maar is ze ook verantwoordelijk voor het aantonen dat de

verwerkingsactiviteiten voldoen aan de in dit beleid opgesomde beginselen inzake bescherming van persoonsgegevens en de vereisten van de AVG (**verantwoordingsplicht**).

Om naleving te kunnen aantonen, zal de Proximus Group informatie en documentatie bijhouden van elke beslissing die wordt genomen en elke maatregel die wordt uitgevoerd om de in dit beleid vastgelegde beginselen inzake verwerking van persoonsgegevens na te leven, onder meer door toepassing van een privacy by design-proces, door een register van verwerkingsactiviteiten bij te houden en door DPIA's uit te voeren en te documenteren waar dit wettelijk vereist is, door technische en organisatorische beveiligingsmaatregelen toe te passen en te documenteren, door een proces voor de melding van inbreuken in verband met persoonsgegevens toe te passen, door de uitoefening van de rechten van de betrokkene te vergemakkelijken, enz. Deze documentatie wordt op verzoek beschikbaar gesteld aan de toezichthoudende autoriteit en dient als bewijs van naleving van de wetgeving inzake bescherming van persoonsgegevens.

Met betrekking tot toezicht en controle past Proximus het systeem toe dat in sectie 4 van dit beleid wordt beschreven.

2.3 Privacy by design-proces

In overeenstemming met het AVG-beginsel van de verantwoordingsplicht[12], moet de Proximus Group kunnen aantonen dat regelgeving inzake bescherming van persoonsgegevens (bv. GDPR, e-Privacyrichtlijn) wordt nageleefd en dat de verwerking van persoonsgegevens in overeenstemming met de toepasselijke wetgeving gebeurt.

De Proximus Group gebruikt een proces (**privacy by design-proces**) om de naleving van de vereisten van de wetgeving inzake bescherming van persoonsgegevens te beoordelen voor elk initiatief waarbij persoonsgegevens worden verwerkt. Het privacy by design-proces zal de Proximus Group in staat stellen om te anticiperen op risico's en gebeurtenissen die een schending van de privacy uitmaken en om deze risico's en gebeurtenissen te beperken voordat ze zich voordoen, zodat de beginselen inzake bescherming van persoonsgegevens correct worden toegepast. Het privacy by design-proces zal er ook voor zorgen dat de Proximus Group in de ontwerpfase van elk systeem, product of proces er rekening mee houdt:

- dat de verwerking van persoonsgegevens voldoet aan de beginselen inzake bescherming van persoonsgegevens;
- welke risico's deze verwerkingsactiviteiten kunnen inhouden voor de rechten en vrijheden van betrokkenen; en
- wat de mogelijke maatregelen zijn om de risico's in te perken en om aan te tonen dat de wetgeving wordt nageleefd.

[12] Het beginsel van de verantwoordingsplicht wordt toegelicht in sectie 2.2.7.

2.4 Data Protection Impact Assessment

Wanneer een verwerkingsactiviteit waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van personen, beoordeelt de Proximus Group het effect van de beoogde verwerkingen op de bescherming van persoonsgegevens. Die beoordeling wordt een gegevensbeschermingseffectbeoordeling of 'Data Protection Impact Assessment' in het Engels (**DPIA**) genoemd.

Een DPIA is minstens in de volgende gevallen vereist:

- In geval van een systematische en uitgebreide beoordeling van de persoonlijke aspecten van een persoon, met inbegrip van profilering;
- In geval van een grootschalige verwerking van bijzondere categorieën van persoonsgegevens;
- In geval van een grootschalige en systematische monitoring van openbaar toegankelijke ruimten;
- In geval van een grootschalige en/of systematische verwerking van telefoon-, internet- of andere communicatiegegevens, metadata of locatiegegevens van of herleidbaar tot natuurlijke personen (bijvoorbeeld Wi-Fi tracking of verwerking van locatiegegevens van reizigers in het openbaar vervoer) wanneer de verwerking niet strikt noodzakelijk is voor een door de betrokkene gevraagde dienst.

De DPIA's bevatten en documenteren ten minste de verplichte elementen als opgesomd in artikel 35.7 AVG.

2.5 Rechten van de betrokkenen

De betrokkenen hebben de volgende rechten ten aanzien van de verwerking van hun persoonsgegevens:

- Het recht om te worden geïnformeerd
- Het recht van inzage
- Het recht op rectificatie
- Het recht op gegevenswissing (**recht op vergetelheid**)
- Het recht op beperking van de verwerking
- Het recht op overdraagbaarheid van gegevens
- Het recht van bezwaar
- Rechten in verband met geautomatiseerde individuele besluitvorming en profilering.

De Proximus Group zal passende procedures en opleidingen ontwikkelen en bijhouden om de bovengenoemde rechten van de betrokkenen uit te voeren en om klachten van betrokkenen over de verwerking van hun persoonsgegevens door de Proximus Group te behandelen.

De Proximus Group moet de gepaste middelen ter beschikking stellen van de betrokkenen opdat deze hun rechten kunnen uitoefenen en hun klachten kunnen indienen.

Wanneer de wet dit vereist, moet de Proximus Group het verzoek van de betrokkene uitvoeren en erop antwoorden binnen de termijn die is vastgesteld in artikel 12.3 van de AVG.

De Proximus Group garandeert dat geen enkele betrokkene het slachtoffer zal worden van vergeldingsmaatregelen of discriminatie ingevolge de uitoefening van zijn rechten in het kader van de AVG of omwille van het indienen van een klacht in verband met de verwerking van zijn persoonsgegevens.

2.6 Toestemming

Zoals uitgelegd in sectie 2.2.1.1 van dit beleid (**principe van rechtmatigheid**), moet de verwerking van persoonsgegevens gebaseerd zijn op een van de wettelijke grondslagen opgesomd in de AVG. De voorafgaande toestemming van de betrokkene maakt een van deze wettelijke grondslagen uit. In het geval de verwerking van persoonsgegevens gebaseerd is op deze wettelijke grondslag zijn er bijkomende vereisten waaraan de toestemming moet voldoen opdat deze geldig is.

Om geldig te zijn, moet de 'toestemming' een vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting van de betrokkene zijn waarmee hij of zij door een verklaring of door een duidelijke bevestigende handeling aangeeft in te stemmen met de verwerking van zijn of haar persoonsgegevens. De toestemming van de betrokkene kan te allen tijde worden ingetrokken.

Om een geldige toestemming te verkrijgen, moet de betrokkene voorafgaand volledig geïnformeerd zijn over de verwerking en zijn instemming - gegeven op een moment dat hij of zij bekwaam is om deze te geven en er geen druk op hem of haar wordt uitgeoefend. Toestemming die werd verkregen onder dwang of op basis van misleidende informatie is geen geldige basis voor de verwerking van persoonsgegevens. Toestemming kan niet worden afgeleid uit het uitblijven van een reactie op een mededeling. De toestemming moet betrekking hebben op alle verwerkingsactiviteiten die voor hetzelfde doeleinde of dezelfde doeleinden worden verricht. Wanneer de verwerking meerdere doeleinden heeft, moet voor al die doeleinden afzonderlijk een specifieke toestemming worden gegeven.

Wanneer de Proximus Group diensten van een informatiemaatschappij (d.w.z. onlinediensten) rechtstreeks aan kinderen verleent, zal ze ervoor zorgen dat ze bij de verwerking van persoonsgegevens toestemming heeft gekregen van diegene die de ouderlijke verantwoordelijkheid voor het kind draagt.

De Proximus Group moet voor elke betrokkene kunnen aantonen dat een geldige toestemming is verkregen voor alle verwerkingsactiviteiten met betrekking tot persoonsgegevens waarvoor de passende rechtsgrond de toestemming van de betrokkene is.

2.7 Verwerking van bijzondere categorieën van persoonsgegevens

De verwerking van bijzondere categorieën van persoonsgegevens[13], zoals persoonsgegevens waaruit de etnische afkomst, de religieuze of levensbeschouwelijke overtuiging, het lidmaatschap van een vakbond of gegevens over de gezondheid[14] blijken, en de verwerking van gerechtelijke gegevens[15] is in beginsel verboden, tenzij in specifieke omstandigheden, bijvoorbeeld wanneer de betrokkene uitdrukkelijk toestemming heeft gegeven voor een dergelijke verwerking.

[13] Zie definitie van "bijzondere categorieën van persoonsgegevens" in Bijlage 1.
[14] Zie definitie van "gegevens met betrekking tot gezondheid" in Bijlage 1.
[15] Zie definitie van "gerechtelijke gegevens" in Bijlage 1.

De specifieke wettelijke voorschriften voor de verwerking van bijzondere categorieën van persoonsgegevens en gerechtelijke gegevens worden onderzocht en gedocumenteerd als onderdeel van het privacy by design-proces.

2.8 Inbreuken in verband met persoonsgegevens

2.8.1 Algemeen

De Proximus Group handhaaft en implementeert een passende procedure voor het beheer van inbreuken in verband met persoonsgegevens[16]. De toezichthoudende autoriteit moet in kennis worden gesteld wanneer bekend is dat er zich een inbreuk in verband met persoonsgegevens heeft voorgedaan die waarschijnlijk een risico voor de rechten en vrijheden van personen inhoudt. In dat geval moet de toezichthoudende autoriteit zonder onnodige vertraging en, indien mogelijk, uiterlijk 72 uur nadat kennis werd genomen van de inbreuk in verband met persoonsgegevens, daarvan in kennis worden gesteld.

Wanneer een inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico voor de rechten en vrijheden van natuurlijke personen inhoudt, moet de Proximus Group de betrokken personen onverwijld in kennis stellen van de inbreuk in verband met persoonsgegevens.

Bovendien is de Proximus Group krachtens de e-Privacy-richtlijn verplicht om bij elke inbreuk in verband met persoonsgegevens in verband met het aanbieden van een openbare elektronische-communicatiedienst uiterlijk 24 uur na de vaststelling van de inbreuk de toezichthoudende autoriteit hiervan in kennis stellen, waar mogelijk. De vaststelling van een inbreuk in verband met persoonsgegevens wordt geacht te hebben plaatsgevonden wanneer de Proximus Group voldoende op de hoogte is van het feit dat zich een beveiligingsincident heeft voorgedaan waarbij persoonsgegevens zijn gecompromitteerd, om een zinvolle kennisgeving te kunnen doen.

Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk negatieve gevolgen zal hebben voor de persoonsgegevens of de privacy van een abonnee of een andere persoon, moet de Proximus Group de abonnee of deze andere persoon ook onverwijld in kennis stellen van de inbreuk in verband met persoonsgegevens.

2.8.2 Continue verbetering

In overeenstemming met haar Bold 2025-strategie zet Proximus zich in voor de bescherming van de privacy en de veiligheid van de persoonsgegevens die het verwerkt. Proximus erkent het belang van een continue verbetering van haar maatregelen inzake bescherming van persoonsgegevens en verbindt zich

[16] Zie definitie van "inbreuken in verband met persoonsgegevens" in Bijlage 1.

ertoe om prioriteiten te stellen en tijdig de nodige structurele verbeteringen door te voeren om het risico op inbreuken in verband met persoonsgegevens, ongeoorloofde toegang, ... te verminderen.

Bovendien begrijpt Proximus dat het landschap op vlak van bescherming van persoonsgegevens voortdurend evolueert en dat er nieuwe uitdagingen kunnen opduiken. In het kader van dit beleid verbindt Proximus zich ertoe om op de hoogte te blijven van de recentste industrienormen, 'best practices' en wettelijke vereisten om ervoor te zorgen dat haar maatregelen inzake bescherming van persoonsgegevens toonaangevend zijn en blijven.

Door deze principes in te voeren en na te leven, geeft Proximus blijk van haar vaste wil om de persoonsgegevens die het verwerkt te beschermen. Dankzij de voortdurende inspanningen om prioriteiten te stellen en structurele verbeteringen door te voeren, streeft Proximus ernaar persoonsgegevens optimaal te beschermen en de hoogste normen op het gebied van gegevensbescherming te handhaven en zo het vertrouwen in haar merk op te bouwen.

2.9 Persoonsgegevens delen

De Proximus Group moet ervoor zorgen dat onbevoegde derden, hetzij intern (d.w.z. binnen de Proximus Group) of extern (d.w.z. buiten de Proximus Group), geen kennis kunnen nemen van persoonsgegevens. Alle medewerkers moeten waakzaam zijn wanneer hen gevraagd wordt persoonsgegevens van een andere persoon aan een derde mee te delen. Hierbij moet men in het achterhoofd houden of het meedelen van deze persoonsgegevens al dan niet relevant en noodzakelijk is voor het uitvoeren van de activiteiten van de Proximus Group.

Ook persoonsgegevens delen maakt een verwerking van persoonsgegevens uit die onderworpen is aan alle beginselen die opgenomen zijn in sectie 2.2 van dit beleid. In het bijzonder vereist het AVG-beginsel van rechtmatigheid dat er een rechtmatige grondslag[17] is voor het delen van persoonsgegevens en dat deze rechtmatige grondslag is gedocumenteerd. Het delen van persoonsgegevens moet altijd onderworpen zijn aan passende beveiligingsmaatregelen[18]. De rechtmatigheid en andere wettelijke beginselen die van toepassing zijn op het delen van persoonsgegevens worden gecontroleerd en gedocumenteerd als onderdeel van het privacy by design-proces.

2.9.1 Uitwisseling van gegevens binnen de Proximus Group

De uitwisseling van persoonsgegevens tussen entiteiten van de Proximus Group moet aan alle vereisten met betrekking tot de uitwisseling van persoonsgegevens voldoen, zoals uitgelegd in deze sectie 2.9.

[17] Het beginsel van rechtmatigheid werd uitgelegd in sectie 2.2.1.1.
[18] Het beginsel van beveiliging van persoonsgegevens werd uitgelegd in sectie 2.2.6.

Bovendien moeten alle Proximus-medewerkers rekening houden met eventuele beperkingen opgelegd door het mededingingsrecht (zie hiervoor het beleid "Concurrentie incl. Chinese Walls, informatie-uitwisselingen en Dawn Raids").

2.9.2 Doorgifte van persoonsgegevens buiten de EU

De Proximus Group verbindt zich ertoe te zorgen voor passende waarborgen ter bescherming van persoonsgegevens die door haar worden doorgegeven aan landen die geen passende wetten inzake bescherming van persoonsgegevens hebben, zoals vereist door de toepasselijke wetgeving.

Bij de doorgifte van persoonsgegevens aan een land dat geen lid is van de Europese Economische Ruimte (**derde land**), dienen een van de volgende instrumenten overeenkomstig hoofdstuk V van de AVG worden gebruikt om een passend niveau van bescherming van persoonsgegevens te waarborgen:

- De erkenning door middel van een besluit van de Europese Commissie van een passende regelgeving inzake bescherming van persoonsgegevens (**adequaatheidsbesluit**) in het land waar de ontvanger van de persoonsgegevens zich bevindt.
- Indien er geen adequaatheidsbesluit is, kan een doorgifte plaatsvinden wanneer passende waarborgen worden geboden. Een voorbeeld van dergelijke passende waarborgen zijn de contractuele afspraken met de ontvanger van de persoonsgegevens, waarbij bijvoorbeeld de door de Europese Commissie goedgekeurde modelcontractbepalingen worden gebruikt.
- Indien ten slotte een doorgifte van persoonsgegevens wordt overwogen naar een derde land waarvoor geen adequaatheidsbesluit voorhanden is en er geen passende waarborgen zijn, kan een doorgifte plaatsvinden op basis van een aantal specifieke uitzonderingsbepalingen, bijvoorbeeld in het geval waarbij een betrokkene uitdrukkelijk heeft ingestemd met de voorgestelde doorgifte na alle nodige informatie over de aan de doorgifte verbonden risico's te hebben ontvangen.

2.9.3 Verwerkers

De Proximus Group zal voor elk standaardproduct/elke standaarddienst de rol van haar respectievelijke entiteit met betrekking tot de verwerking van persoonsgegevens (d.w.z. verwerkingsverantwoordelijke of verwerker[19]) vastleggen en ervoor zorgen dat de juiste contractuele bepalingen worden opgenomen die de verantwoordelijkheden en verplichtingen in verband met die rol weerspiegelen.

Indien een entiteit van de Proximus Group of van een andere partij die diensten verleent aan de Proximus Group als verwerker optreedt, zal de door de partijen gesloten overeenkomst de verplichtingen van de verwerker tegenover de verwerkingsverantwoordelijke in overeenstemming met artikel 28 van de AVG (**verwerkersovereenkomst**).

[19] Zie definities van 'verwerkingsverantwoordelijke' en 'verwerker' in Bijlage 1.

2.9.4 Gezamenlijke verwerkingsverantwoordelijken

Indien een entiteit van de Proximus Group persoonsgegevens verwerkt als gezamenlijk verwerkingsverantwoordelijke[20] samen met een of meer andere organisaties, moet zij een overeenkomst aangaan met die organisatie(s) waarin de respectieve verantwoordelijkheden voor de naleving van de AVG-voorschriften worden vastgelegd. De belangrijkste aspecten van deze overeenkomst moeten aan de betrokkenen worden meegedeeld.

2.10 Opleiding en sensibilisering

De Proximus Group zal opleidings- en sensibiliseringsprogramma's bevorderen en middelen ter beschikking stellen om het bewustzijn te vergroten en algemene en specifieke opleidingen over de bescherming van persoonsgegevens te verstrekken die relevant zijn voor de dagelijkse taken en verantwoordelijkheden. De Proximus-medewerkers moeten alle vereiste opleidingen inzake bescherming van persoonsgegevens en informatiebeveiliging volgen en voltooien.

2.11 Register van verwerkingsactiviteiten

In lijn met artikel 30 AVG en teneinde erover te waken dat de Proximus Group de persoonsgegevens die het verwerkt, de doeleinden waarvoor het deze verwerkt en het risiconiveau i.v.m. de verwerking van deze informatie begrijpt, zal de Proximus Group een register van verwerkingsactiviteiten bijhouden waarin alle activiteiten m.b.t. de verwerking van persoonsgegevens beheerd onder de verantwoordelijkheid van Proximus, in de hoedanigheid van verwerkingsverantwoordelijke, gezamenlijke verwerkingsverantwoordelijke en de verwerker, worden gedocumenteerd.

3. Policy: Elektronisch communicatiegeheim

3.1 Principe

De vertrouwelijkheid van de elektronische communicatie beveiligt de inhoud van oproepen en elektronische communicatiegegevens, zoals opgeroepen nummers, de duur van de communicatie, de internetverbinding, en de vertrouwelijkheid van privénummers (**elektronische communicatiegegevens**[21]). Zowel de inhoud van een communicatie als de gegevens betreffende de communicatie moeten vertrouwelijk worden behandeld.

[20] Zie definitie van 'gezamenlijke verwerkingsverantwoordelijke' in Bijlage 1.
[21] Zie definitie van 'elektronische communicatiegegevens' in Bijlage 1.

Bescherming van de communicatie-inhoud

Een persoon die niet aan een communicatie (zijnde een mobiele, vaste of gegevenscommunicatie) deelneemt, mag de inhoud van de verstuurde communicatie niet proberen consulteren. Daarnaast is het verboden om de inhoud van de communicatie op te nemen.

Bescherming van de gegevens i.v.m. de communicatie

Het is verboden om met opzet gegevens inzake elektronische communicatie m.b.t. andere personen te achterhalen, openbaar te maken, te wijzigen of te vernietigen, of om de betrokken personen te identificeren.

3.2 Uitzonderingen

Enkele situaties waarbij dit verbod niet van toepassing is op een telecomoperator en zijn medewerkers worden bij wet gedefinieerd (zie niet-exhaustieve lijst hieronder).

Neem contact op met de bevoegde adviseur van het juridische departement om na te gaan een van de uitzonderingen van toepassing is. Voorbeelden van uitzonderingen:

- Noodzakelijkheid om het netwerk te controleren om de behoorlijke werking ervan te verzekeren of om te verzekeren dat de telecommunicatiedienst naar behoren wordt geleverd;
- Er werd toestemming verleend door alle partijen die aan de communicatie deelnemen;
- De metadata met betrekking tot de elektronische communicatie (niet de inhoud van de communicatie) worden gebruikt voor de volgende specifieke doelen:
    - facturatie en interconnectiebetaling;
    - direct marketing met de toestemming van de klant;
    - aanbieden van tracking- en trafiekdatadiensten;
    - trafiekmanagement;
    - fraudedetectie.

Er zijn ook wettelijke uitzonderingen op het elektronische communicatiegeheim voor de gerechtelijke instanties, de hulpdiensten, het Belgisch Instituut voor Postdiensten en Telecommunicatie, de Ombudsdienst voor Telecommunicatie.

Bovendien zijn er ook wettelijke uitzonderingen die het opnemen van communicaties toelaten om kwaliteitscontrole in callcenters mogelijk te maken en als bewijs te dienen van commerciële transacties.

3.3 Gevolgen in geval van niet-naleving

Elk geval waarbij de ePrivacy Richtlijn niet wordt nageleefd, kan aanleiding geven tot boetes tot € 800.000 en gevangenisstraffen tot 4 jaar.

4. Monitoring en controle

Om te controleren of de Proximus Group de wetgeving inzake bescherming van persoonsgegevens naleeft, zal de Proximus Group:

- een kader met passende interne controles en onafhankelijke toezichtsmechanismen handhaven om toe te zien op de naleving van de toepasselijke wetgeving, de procedures en het beleid inzake bescherming van persoonsgegevens; en
- een privacy by design-proces ontwikkelen, handhaven en toepassen zodat initiatieven rond nieuwe producten en diensten waarbij persoonsgegevens verwerkt worden, plaatsvinden in overeenstemming met de vereisten inzake bescherming van persoonsgegevens;
- ad hoc controles m.b.t. de naleving van de richtlijnen van de toezichthoudende autoriteit uitvoeren;
- ad hoc audits door interne of externe 'trusted' auditors laten uitvoeren.

Bijlage 1: Definities

AVG (Algemene Verordening Gegevensbescherming) – Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van de Richtlijn 95/46/EG.

Betrokkene – Elk levend individu dat het onderwerp is van persoonsgegevens die door een organisatie worden bijgehouden.

Bijzondere categorieën van persoonsgegevens - Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens met betrekking tot gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid

Biometrische gegevens - Persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens

Derde - Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken.

Elektronische communicatiegegevens – Verkeersgegevens en locatiegegevens. Verkeersgegevens zijn alle gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronisch communicatienetwerk of voor de facturering daarvan. Locatiegegevens zijn alle gegevens die worden verwerkt in een elektronische-communicatienetwerk waarmee de geografische positie van de eindapparatuur van een gebruiker van een openbare elektronische-communicatiedienst wordt aangegeven.

ePrivacy Richtlijn (Richtlijn inzake privacy en elektronische communicatie) – Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie, in het bijzonder de eerbiediging van het privéleven, de vertrouwelijkheid van de communicatie en de bescherming van persoonsgegevens in de sector elektronische communicatie. De richtlijn is in Belgisch recht omgezet bij de wet van 13 juni 2005 betreffende de elektronische communicatie.

Gegevens met betrekking tot gezondheid - Persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven

Genetische gegevens - Persoonsgegevens die verband houden met de overgeërfde of verworven genetische kenmerken van een natuurlijke persoon die unieke informatie verschaffen over de fysiologie of de gezondheid van die natuurlijke persoon en die met name voortkomen uit een analyse van een biologisch monster van die natuurlijke persoon

Gezamenlijke verwerkingsverantwoordelijke – Een verwerkingsverantwoordelijke die samen met een of meer andere verwerkingsverantwoordelijken het doel en de middelen van de verwerking van persoonsgegevens bepaalt.

Inbreuk in verband met persoonsgegevens - Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens

Gerechtelijke gegevens - Persoonsgegevens met betrekking tot strafrechtelijke veroordelingen en overtredingen of daarmee verband houdende veiligheidsmaatregelen.

Kind – De AVG definieert een kind als iedereen die jonger is dan 16 jaar. De verwerking van persoonsgegevens van een kind jonger dan 13 jaar is alleen rechtmatig indien toestemming van de ouders of de voogd werd verkregen.

Persoonsgegevens - Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ('de betrokkene'); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon

Profilering - Elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen. Deze definitie is gekoppeld aan het recht van de betrokkene om zich tegen profilering te verzetten en het recht om geïnformeerd te worden over het bestaan van profilering, over maatregelen die gebaseerd zijn op profilering en over de beoogde gevolgen van profilering voor de betrokkene.

Toestemming van de betrokkene - Elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt.

Toezichthoudende autoriteit (Gegevensbeschermingsautoriteit) - Een door een lidstaat ingestelde onafhankelijke overheidsinstantie. In België is dit de 'Gegevensbeschermingsautoriteit'/ 'L'Autorité de protection des données' ofwel de 'Toezichthoudende Autoriteit'.

Verwerker - Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

Verwerking – Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens

Verwerkingsverantwoordelijke - Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze

verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen

Vestiging – De hoofdvestiging van de verwerkingsverantwoordelijke in de EU is de plaats waar de verwerkingsverantwoordelijke de belangrijkste beslissingen neem over het doel en de middelen van de verwerkingsactiviteiten. De hoofdvestiging van de verwerkingsverantwoordelijke in de EU is de plaats van zijn centrale administratie. Indien een verwerkingsverantwoordelijke buiten de EU is gevestigd, moet hij een vertegenwoordiger benoemen in het rechtsgebied waar hij actief is, die namens de verwerkingsverantwoordelijke optreedt en met de toezichthoudende autoriteiten in contact staat.