Intern Privacybeleid

Het Privacybeleid geeft inzicht in de verwerking van persoonsgegevens binnen de onderneming.

PYRAMID NV

PYRAMID NV

Tel +32 9 324 70 80

Lambroekstraat 5A
1831 Diegem

Inhoud

I. Inleiding

I.I Introductie

In dit Privacybeleid laat **PYRAMID NV** zien op welke manier zij omgaat met de verwerking van persoonsgegevens.

Digitale innovaties, zoals smartphones, computers, GPS, Internet of Things… maken onze huidige werkomgeving aangenamer en zorgen voor een efficiëntere werking van onze onderneming. Anderzijds zorgt het gebruik van nieuwe technologieën ervoor dat persoonsgegevens op grote schaal worden verwerkt.

Met de komst van de Algemene Verordening Gegevensbescherming (Afgekort 'AVG' maar beter gekend onder de 'General Data Protection Regulation' hierna 'GDPR') die in werking treedt op 25 mei 2018 krijgen bedrijven een grotere rol toebedeeld inzake de interne controle op de rechtmatige verwerking van persoonsgegevens. Een onderneming komt namelijk dagelijks in contact met gegevens van personen en is een 'Verwerkingsverantwoordelijke'.

PYRAMID NV ziet het als een opportuniteit om een weldoordachte verwerking van persoonsgegevens door te voeren en zo het vertrouwen in de onderneming te versterken.

Dit document is een beleid waarin de richting wordt aangegeven en een structuur wordt aangereikt waarmee ons bedrijf de wettelijke en nuttige operationele werking inzake verwerking van persoonsgegevens zal weergeven en verder versterken.

I.II Doelstelling

PYRAMID NV levert inspanningen om de verwerking van persoonsgegevens op de meest behoorlijke wijze te laten verlopen. Dit wil zeggen dat persoonsgegevens worden verwerkt op basis van een legitieme grondslag, voor een welbepaald doel, op een transparante manier en dit op een proportionele wijze.

Dit betekent het volgende:

- Informatie van klanten, kandidaten en gegevens van PYRAMID NV en dochterondernemingen zelf met de grootst mogelijke zorg veilig afgeschermd beheren en bewaren.
- Algemeen bewustzijn rond het belang van informatiebeveiliging en verwerking persoonsgegevens verhogen.
- Zorgen voor “business continuity”
- Mogelijke risico’s op incidenten en de impact ervan te minimaliseren.

I.III Reikwijdte

PYRAMID NV bestaat uit volgende bedrijven/afdelingen:

- Pauwels Consulting NV
- Pauwels Consulting France SARL
- PIT Advisor NV
- Akros Solutions SPRL
- Akros Europe SPRL
- Mediconsult V.D. International BVBA

I.IV Implementatie

Dit document is het beleid omtrent bescherming van persoonsgegevens. De implementatie wordt opgesplitst in vier onderdelen:

- Bewustmakingsproces van alle personen binnen PYRAMID NV voor verwerking van persoonsgegevens;
    - Er wordt door PYRAMID NV een dataregister bijgehouden met alle verwerkingsactiviteiten inzake persoonsgegevens;
    - Dit beleid wordt kenbaar gemaakt in de onderneming;

- Het nemen van preventieve maatregelen;
    - Beveiligingsmaatregelen worden geïmplementeerd in de werking van de onderneming;
    - Door het identificeren van verwerkingen die een hoog risico vormen waarvoor een Gegevensbeschermingseffectenbeoordeling opgesteld. Hierbij worden de aanbevelingen van de Privacycommissie nauwgezet opgevolgd;
    - De overeenkomsten met externe verwerkers en externe overeenkomsten worden gecontroleerd op hun overeenstemming met de GDPR;

- Evaluatiemomenten worden ingepland;
- Herstellingsmaatregelen worden toegepast en geëvalueerd;
    - Bij datalekken wordt de procedure gevolgd zoals hieronder wordt beschreven;
    - Jaarlijks wordt een rapport opgemaakt door de Data Protection Officer betreffende de uitvoering van het beleid, eventuele aanpassingen en het aantal procedures die werden toegepast.

Pauwels Management BVBA, Gedelegeerd Bestuurder, Vertegenwoordigd door Bert Pauwels
25 mei 2018

II. Wet – en regelgeving

II.I Europese wetgeving: De Algemene Verordening Gegevensbescherming of General Data Protection Regulation 'GDPR'.

De Algemene Verordening Gegevensbescherming ("GDPR" beter gekend onder General Data Protection Regulation "GDPR") dateert van 24 mei 2016, maar bedrijven en organisaties krijgen tot **25 mei 2018** de tijd om zich aan de nieuwe eisen van de GDPR aan te passen. Onder dit hoofdstuk worden de punten kort samengevat en in de volgende hoofdstukken wordt het beleid aangaande deze stukken uitgewerkt.

De volledige verordening kan u terugvinden op volgende link: http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32016R0679

Naast deze verordening is er ook de **nieuwe e-privacy verordening.** Deze handelt voornamelijk over elektronische communicatiegegevens.

***De GDPR stelt volgende hoofdspelers voorop**:*

- De **Betrokkene**: het individu waarover de informatie wordt verwerkt.
- De **Verwerkingsverantwoordelijke**: organisatie die gegevens verwerkt en het doel en de middelen van de verwerking bepaalt.
- **Verwerker**: Diegene die ten behoeve van de Verwerkingsverantwoordelijke gegevens verwerkt;
- **De toezichthoudende autoriteit**. Dit is op heden de 'Belgische Privacycommissie'. Deze Privacycommissie wordt omgevormd tot de 'Belgische Gegevensbeschermingsautoriteit'. Er is een mogelijkheid om klacht in te dienen bij de toezichthoudende autoriteit wanneer gegevens foutief worden verwerkt;

Door de Privacycommissie werden richtlijnen opgesteld over hoe een onderneming zich kan conformeren aan de komende verordening. Het privacybeleid is opgesteld conform deze richtlijnen en zorgt voor de nodige beschermings- en risicoanalyses waar nodig. Daarnaast worden ook de documenten van de 'Article 29 Working Party' van de Europese Unie opgevolgd om zoveel als mogelijk de persoonsgegevens te beschermen. Deze aanbevelingen worden gepubliceerd op volgend adres: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 .

De GDPR hanteert volgende principes voor de verwerking van persoonsgegevens:

- Er moet sprake zijn van **een rechtmatige, behoorlijke en transparante verwerking**; alle informatie of elke communicatie met betrekking tot de verwerking van de gegevens moet gemakkelijk toegankelijk en te begrijpen zijn;

- Voor **welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden**; Opmerking: de GDPR rechtvaardigt de verwerking voor andere doeleinden dan de initiële indien de verwerking verenigbaar is met de doeleinden waarvoor de gegevens initieel zijn verzameld – evaluatie van de verenigbaarheid dient te gebeuren door de verwerkingsverantwoordelijke; De verenigbaarheid is niet vereist indien er een juridische basis is voor de verwerking en toestemming door Europees of nationaal recht;

- Gegevens moeten **nauwkeurig en juist** zijn en indien nodig up-to-date worden gebracht, een correctie van de gegevens is mogelijk;

- De gegevensverwerking wordt **beperkt tot wat noodzakelijk** is, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt;

- **De bewaartermijn van de persoonsgegevens is beperkt** tot zolang als nodig met betrekking tot de doeleinden. De gegevens moeten in een vorm worden bewaard die het mogelijk maakt de betrokkenen niet langer te identificeren dan

voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is;

- **Integriteit en vertrouwelijkheid** , de verwerking moet passend beveiligd worden middels passende technische of organisatorische maatregelen;

Welke activiteiten vallen onder de verordening?

De verordening is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking, alsmede op de niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Het materiële toepassingsgebied is niet veranderd ten aanzien van de oude richtlijn.

De verwerking bestaat uit de volgende handelingen met persoonsgegevens:

- Het verzamelen, vastleggen en ordenen;
- Het bewaren, bijwerken, structureren of wijzigen;
- Het opvragen, raadplegen, gebruiken;
- Het verstrekken door middel van doorzending;
- De verspreiding of enige andere vorm van ter beschikkingstellen;
- Het samenbrengen, met elkaar in verband brengen;
- Het afschermen, uitwissen of vernietigen;

Territoriaal?

1. De verwerkingsverantwoordelijke is gevestigd in de Europese Unie ambtshalve toepassing van de verordening

2. De verwerkingsverantwoordelijke is gevestigd buiten de Europese Unie. Wanneer in dat geval de verwerkingsactiviteiten betrekking hebben op het aanbieden van goederen of diensten aan die personen hetzij betrekking hebben op het observeren van het gedrag van de betrokkenen binnen de Europese Unie dan is de verordening van toepassing.

In volgende hoofdstukken wordt uiteengezet hoe de persoonsgegevens worden verwerkt in overeenstemming met de GDPR.

II.II De Belgische Wetgeving

Op heden geldt de huidige wetgeving inzake de Belgische Wet Verwerking Persoonsgegevens van 8 december 1992 zoals gewijzigd op 11 december 1998. Deze wijziging kwam er na de eerste richtlijn Gegevensbescherming van 1995. De basisprincipes van de oude richtlijn en dus Belgische wet werden behouden maar in de GDPR worden deze versterkt en genuanceerd.

De volledige wet kan u op dit adres raadplegen:

https://www.privacycommission.be/sites/privacycommission/files/documents/privacy_nl_0.pdf

De Privacycommissie wordt hervormd naar de Belgische Gegevensbeschermingsautoriteit (hierna BGA). De tekst werd aangenomen door de Kamer van Volksvertegenwoordigers op 9 november 2017. De autoriteit wordt opgericht en de overige bepalingen van de wet treden in werking op 25 mei 2018.

Wat is de Belgische Gegevensbeschermingsautoriteit?

Er worden binnen de GBA 6 organen opgericht:

1. Een directiecomité
2. Een algemeen secretariaat
3. Een eerstelijnsdienst
4. Een kenniscentrum
5. Een inspectiedienst
6. Een geschillenkamer

Wat kan de GBA allemaal doen?

- Informatie en advies verlenen aan particulieren, verwerkingsverantwoordelijken (en hun verwerkers) en aan de overheid om de wetgeving inzake gegevensbescherming na te leven of te doen naleven.

- Begeleiding van de verwerkingsverantwoordelijken (en hun verwerkers) bij het maximaal benutten van preventieve instrumenten in de GDPR zoals certificering (momenteel is deze certificering er nog niet) naleving van gedragscodes, indicaties voor het aanstellen van een Data Protection Officer.

- Controle op de naleving van de GDPR door de verwerkingsverantwoordelijken (en hun verwerkers) door een daarvoor specifiek opgeleide inspectiedienst.

- Het uitdelen van sancties – variërend van waarschuwingen tot financiële sancties bij slechte leerlingen – dit wordt geval per geval beoordeeld en naargelang de ernst van de situatie wordt een evenwichtige en proportionele behandeling voor te stellen.

De gewijzigde nationale wetgeving is nog niet officieel van kracht en wordt verwacht in juni 2018.

III. Verwerking van Persoonsgegevens binnen PYRAMID NV

III.I Welke Persoonsgegevens zijn er aanwezig binnen PYRAMID NV?

1. Algemeen

Persoonsgegevens zijn:

'Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon; als identificeerbaar wordt beschouwd een natuurlijk 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.'

Alle gegevens waarmee je kan aanduiden wie de persoon is of die aanleiding geven tot het aanduiden van een individu zijn gegevens die op een behoorlijke manier en conform met de GDPR verwerkt moeten worden.

PYRAMID NV houdt een dataregister bij met alle verwerkingen van persoonsgegevens. Dit register wordt twee maal per jaar geëvalueerd en geüpdatet.

De categorieën van persoonsgegevens worden opgesomd in het dataregister dat ter beschikking wordt gesteld van de onderneming en aan de Belgische Gegevensbeschermingsautoriteit wanneer hiernaar wordt verzocht. Dit is een interne documentatie van de verwerkingsactiviteiten die door PYRAMID NV werden verricht.

Zo is er een overzicht van de persoonsgegevensverwerkingen die wij verrichten en kunnen wij deze identificeren. Zij worden ingedeeld in verschillende categorieën.

De eerste reeks categorieën zijn de dagdagelijkse persoonsgegevens. Die worden opgesteld met de normale bedrijfswerking in gedachten maar ze zijn niet exhaustief.

Daarnaast hebben we een aantal bijzondere categorieën van persoonsgegevens die uit hun aard 'gevoelige' persoonsgegevens zijn. De verwerking van deze gegevens is in principe verboden behalve in door de wet voorziene uitzonderingen (infra…).

2. **Gewone categorie persoonsgegevens;**

- Contactgegevens (naam, adres, telefoon, e-mail, aanspreektitel, geslacht, social media ids, functie, etc.)
- Identificatiegegevens, andere dan het rijksreg.nr. uitgegeven door overheid: Id-nr. Paspoort, rijbewijs, Pensioennr. , nummerplaat
- Elektronische identificatiegegevens en lokalisatie (IP-adressen, cookies, verbindingsmomenten, GPS, GSM)
- Overheidsgegevens (rijksregisternummer)
- Financiële informatie (bankgegevens, lonen, leningen, beleggingen, groepsverzekeringen, pensioenen, etc.)
- Persoonlijke eigenschappen (leeftijd of geboortedatum, etc.)
- Fysieke eigenschappen (lengte, gewicht, schoenmaat, kleur van ogen, …)
- Opleiding en diploma's
- Loopbaangegevens (Cv's)
- Hobby's en interesses
- Consumptiegewoonten

3. **Bijzondere categorie van persoonsgegevens**;

- Ras of etnische afkomst
- Politieke voorkeur
- Religieuze of levensbeschouwelijke voorkeur
- Lidmaatschappen van verenigingen, vakbonden, etc.
- Genetische gegevens
- Biometrische gegevens met het oog op identificatie
- Gegevens over gezondheid
- Gegevens met betrekking tot seksueel gedrag of seksuele gerichtheid

III.II Toepassing van de principes in lijn van de GDPR op de verwerking van persoonsgegevens

1. Een rechtmatige behoorlijke en transparante verwerking;

Alle informatie of elke communicatie met betrekking tot de verwerking van de gegevens moet gemakkelijk toegankelijk en te begrijpen zijn;

PYRAMID NV hanteert steeds één van de volgende rechtsgronden voor de gewone categorieën van persoonsgegevens:

a) Toestemming van de betrokkene:
De toestemming van de betrokkene is het akkoord dat de betrokkene partij geeft met de vraag om de persoonsgegevens van de betrokkene te verwerken.

De toestemming is:

- Vrij
- Geïnformeerd en specifiek
- Ondubbelzinnig

De toestemming dient steeds vrij te worden gegeven.

b) Contractuele reden:
Wanneer de verwerking van gegevens noodzakelijk is voor de uitvoering van een overeenkomst of voor de uitvoering van precontractuele maatregelen op verzoek van de betrokkene;

c) Wettelijke verplichting
Verschillende wetten en uitvoeringsbesluiten maken het verwerken van Persoonsgegevens noodzakelijk om aan de verplichtingen als onderneming te voldoen.

d) **Vitaal belang van betrokkene of ander betrokkene**
Het vitaal belang of levensbelang van de betrokkene impliceert dat de verwerking van gegevens van levensbelang is om de persoon in kwestie te helpen indien betrokkene fysiek of juridisch niet in staat is toestemming te geven. Bijvoorbeeld als iemand bewusteloos wordt gevonden en een ambulance wordt opgebeld en de gegevens van de betrokkene worden doorgestuurd.

e) **Algemeen belang of uitoefening openbaar gezag**
Het kan noodzakelijk zijn voor het Algemeen belang dat persoonsgegevens worden verwerkt.

f) **Gerechtvaardigde Belangen van de Verwerkingsverantwoordelijke (legitiem belang) of van een derde die in de lijn van het doel van de verwerking liggen**
Verwerking is noodzakelijk voor behartiging van de gerechtvaardigde belangen van verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en fundamentele vrijheden van de betrokkene dit tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen.

Voor de bijzondere Categorieën van persoonsgegevens geldt een verwerkingsverbod behalve wanneer;

a) Er **uitdrukkelijk**e toestemming werd gegeven;

b) De verwerking noodzakelijk is voor de uitvoering van verplichting en uitoefening van specifieke rechten van de verwerkingsverantwoordelijke of betrokkenen op gebied van **het arbeidsrecht en sociale zekerheids- en sociale beschermingsrecht** (zolang Unierecht of Lidstatelijk recht of bij collectieve overeenkomst waarborgen worden gegeven voor de grondrechten);

c) **het vitaal belang** van betrokkene of andere persoon primeert indien betrokkene fysiek of juridisch niet in staat is toestemming te geven;

d) Het gaat over een **Stichting, vereniging of andere instantie zonder winstoogmerk**, die op p**olitiek, levensbeschouwelijk, godsdienstig of vakbondsgebied** werkzaam is

e) **het openbare gegevens betreffen**: Gegevens die door de betrokkene openbaar zijn gemaakt

f) **het gegevens voor justitie betreffen**: noodzakelijk voor instelling uitoefening of onderbouwing van een rechtsvordering of wanneer gerechten handelen in het kader van hun rechtsbevoegdheid

g) **er sprake is van een zwaarwegend algemeen belang**, op grond van Unierecht of het lidstatelijk recht waarbij evenredigheid met nagestreefde doel wordt gewaarborgd en specifieke maatregelen worden getroffen ter bescherming van grondrechten en fundamentele belangen; ·

h) wanneer de verwerking noodzakelijk is voor doeleinden van **preventieve of arbeidsgeneeskunde**

i) wanneer de verwerking noodzakelijk is voor het algemeen belang op het gebied van **volksgezondheid,** zoals beschermen tegen ernstige grensoverschrijdende gevaren voor de gezondheid, of waarborgen, normen, kwaliteit en veiligheid van de gezondheidszorg en van geneesmiddelen of medische hulpmiddelen

j) de verwerking noodzakelijk is met oog op **archivering** in het algemeen belang, **wetenschappelijk of historisch onderzoek of** statistische doeleinden overeenkomstig artikel 89, lid 1, op grond van Unierecht of lidstatelijk recht, evenredigheidstoets met specifieke maatregelen

2. Voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden;

Het dient voor de betrokkenen duidelijk te zijn voor welk doel hun gegevens worden verwerkt. Deze doelen moeten zo specifiek mogelijk worden gedefinieerd.

Opmerking: De GDPR rechtvaardigt de verwerking voor andere doeleinden dan de initiële indien de verwerking verenigbaar is met de doeleinden waarvoor de gegevens initieel zijn verzameld – evaluatie van de verenigbaarheid dient te gebeuren door de verwerkingsverantwoordelijke, de onderneming doet dit in overleg met de Data Protection Officer.

De verenigbaarheid is niet vereist indien er een juridische basis is voor de verwerking en toestemming vanwege Europees of nationaal recht;

In het dataregister worden volgende doeleinden nader bepaald, deze doeleinden zijn een niet-exhaustieve opsomming:

- Administratie van het personeel en de tussenpersonen
- Beheer van het personeel en de tussenpersonen
- Werkplanning
- Controle op de werkplaats
- Klantenbeheer
- Bestrijding van fraude en inbreuken van het cliënteel
- Beheer van de betwistingen
- Leveranciersbeheer
- Verzamelen van giften
- Public relations
- Technisch-commerciële inlichtingen
- Registratie en administratie van aandeelhouders of vennoten
- Ledenadministratie
- Beveiliging
- Beheer van geschillen
- Bescherming van de maatschappij, eigen sector of organisatie

3. **De persoonsgegevens moeten nauwkeurig en juist worden verwerkt;**

   De gegevens moeten nauwkeurig en juist worden verwerkt, de betrokkene staat in voor het juist meedelen van deze gegevens en hij dient de onderneming tijdig op de hoogte te brengen bij eventuele wijzigingen.

   De betrokkenen kunnen hun gegevens wijzigen door de bevoegde personen te contacteren.

4. **De gegevensverwerkingen en hun bewaartermijn worden beperkt tot wat noodzakelijk is, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt;**

   De bewaartermijn van de persoonsgegevens is beperkt tot zolang als nodig met betrekking tot de doeleinden;

   De bewaartermijn kan specifiek worden bepaald, maar in de gevallen waarin dit niet mogelijk zou zijn, worden deze gegevens zolang bewaard als nodig. Dit natuurlijk in overweging met de rechten van de betrokkene.

5. **Integriteit en vertrouwelijkheid**;

   De verwerking moet passend beveiligd worden middels passende technische of organisatorische maatregelen; De principes van Privacy by Design worden waar mogelijk toegepast om de persoonsgegevens te beschermen, dit betekent dat waar mogelijk in standaardinstellingen de privacy zoveel als mogelijk wordt gewaarborgd.

   De organisatorische maatregelen worden verder in dit beleid uiteengezet. Elke werknemer, medewerker, elk deel van de organisatie levert de nodige inspanningen om dit beleid zoveel als mogelijk te implementeren.

III.III Worden de gegevens aan externen verschaft?

PYRAMID NV zal de persoonsgegevens uitsluitend verstrekken aan verwerkers of gelieerde vennootschappen indien dit nodig is voor de uitvoering van de overeenkomst met de betrokkene of om te voldoen aan een wettelijke verplichting of wanneer het legitiem belang van de onderneming dit vereist en dit verenigbaar is met het doel van de verwerking en dit op een proportionele wijze gebeurt.

Met bedrijven die gegevens verwerken in onze opdracht, sluiten wij een verwerkersovereenkomst of levert de overeenkomst tussen de partijen voldoende waarborgen om te zorgen voor eenzelfde niveau van beveiliging en vertrouwelijkheid van uw gegevens. De GDPR stelt over de GDPR het volgende.

Gegevensstroom binnen Europese Economische Ruimte (EER) is toegestaan. Alle Europese lidstaten worden geacht een passend beschermingsniveau te waarborgen

Indien de gegevensstroom van EER naar niet-EER zou gaan moet het adequaatsheidsbesluit van de Europese Commissie worden bekeken. Heeft het land waarnaar de gegevens worden verstuurd geen adequaatheidsbesluit dan moet men als bedrijf zelf de waarborgen geven, binnen de bedrijfsvoorschriften en een policy hanteren om dit de nodige waarborgen te geven en te zorgen voor een passende bescherming. Modelcontracten kunnen worden gevonden op http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm

De passende waarborgen zijn de volgende:

- Bindende bedrijfsvoorschriften;
- Standaardbepalingen Europese Commissie;
- Contractbepalingen goedgekeurd door de Privacycommissie;
- Goedgekeurde gedragscode of certificeringsmechanisme;
- Uitdrukkelijke toestemming van de betrokkene;
- Noodzakelijk voor de uitvoering van een overeenkomst;

III.IV Risk based approach – benadering en PIA

De GDPR zorgt voor de verplichting om in bepaalde gevallen over te gaan tot een gegevensbeschermingseffectbeoordeling of Privacy impact assement 'PIA'.

Wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk **een hoog risico** inhoudt voor de rechten en vrijheden van natuurlijke personen voert de verwerkingsverantwoordelijke vóór de verwerking **een beoordeling uit van het effect** van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens.

Eén beoordeling kan een reeks vergelijkbare verwerkingen bestrijken die vergelijkbare hoge risico's inhouden. Het advies van de Data Protection Officer wordt hierbij ingewonnen.

Deze kan hierbij gebruik maken van een combinatie van enerzijds de richtlijnen van de toezichthouders en anderzijds gekende risicolijsten en methodes om een gepaste risico-evaluatie te verrichten, in het licht van de verwerkingen van de verantwoordelijke.

De richtlijnen van de toezichthouders houden rekening met de diverse bepalingen in de GDPR die een op risico gebaseerde aanpak inhouden ("risk based approach").

In een aparte bijlage kan u de aanpak van de PIA terugvinden en het model PIA dat bij verwerkingsactiviteiten met een hoog risico gehanteerd dient te worden.

III.V Rechten van de betrokkenen

De algemene Verordening Gegevensbescherming wil een transparante en duidelijke communicatie ten aanzien van de betrokkene bereiken.

De Algemene Verordening Gegevensbescherming bepaalt dat de betrokkenen een aantal rechten hebben. Deze rechten zijn niet absoluut, PYRAMID NV verbindt er zich toe zoveel als mogelijk en met evenwicht aan belangen deze rechten te waarborgen. Het betreft volgende rechten:

1) Informatie en toegang tot persoonsgegevens;

De betrokkene kan zich informeren omtrent volgende zaken:

- de doeleinden van de verwerking
- de categorieën persoonsgegevens;
- de ontvangers of categorieën van ontvangers aan wie de persoonsgegevens werden of worden verstrekt, en meer bepaald de ontvangers gevestigd in het buitenland of internationale organisaties;
- de bewaartermijn of, als dat niet mogelijk is, de criteria ter bepaling van die termijn;
- het bestaan van het recht om aan de verwerkingsverantwoordelijke te vragen uw persoonsgegevens te verbeteren of te wissen, of de verwerking van uw persoonsgegevens te beperken, of nog het recht om bezwaar te maken tegen die verwerking;
- het recht om klacht in te dienen bij een toezichthoudende autoriteit;
- de bron van de gegevens bij een onrechtstreekse inzameling;
- het bestaan van een geautomatiseerde beslissing, waaronder ook profilering en nuttige informatie over de onderliggende logica ervan, hoe belangrijk de verwerking van uw gegevens is en welke gevolgen dit voor u kan hebben.

Dit verzoek is kosteloos. Voor bijkomende kopieën kan een administratieve vergoeding worden aangerekend. Doet u uw verzoek via elektronische weg, dan ontvangt de betrokkene de informatie elektronisch.

Procedure bij recht op informatie, toegang en correctie

1. Ontvangen van een verzoek van de Betrokkene

In de externe privacyverklaring wordt omschreven op welke manier de Betrokkene een inzage en/of correctieverzoek kan indienen. Dit gebeurt bij PYRAMID NV door verzending naar een specifiek e-mailadres: gdpr@pauwelsconsulting.com.

2. Identificatieplicht

De Organisatie dient eerst de identiteit van de Betrokkene vast te stellen vooraleer gehoor wordt gegeven aan het verzoek van de Betrokkene.

3. Termijn waarop het antwoord gegeven moet worden

PYRAMID NV reageert binnen 1 maand en tracht afdoende binnen de 1 maand te antwoorden tenzij deze zaken complex zijn. In geval het een complex verzoek betreft, bv. door de grote hoeveelheid persoonsgegevens, kan deze termijn worden verlengd.

4. Weigering van een verzoek?

In bepaalde en uitzonderlijke gevallen kan PYRAMID NV weigeren om gehoor te geven aan een verzoek. Dit kan bijvoorbeeld het geval zijn bij een kennelijk ongegronde of buitensporige vraag of wanneer de gerechtvaardigde belang van de onderneming opweegt tegen de belangen van de betrokkene.

5. Antwoord op het verzoek?

PYRAMID NV tracht zoveel als mogelijk gepast te antwoorden op het verzoek van de betrokkene. Tenzij dit onmogelijk blijkt of onevenredig veel inspanning vergt.

2) Correctie en uitwissing van de gegevens

Betrokkene kunnen verzoeken hun gegevens te wissen. PYRAMID NV komt hier in de mate van het mogelijke aan de vraag tegemoet. De betrokkene kan dit vragen wanneer:

- uw gegevens niet langer nodig zijn voor de doeleinden,
- u uw toestemming waarop de verwerking berust, intrekt en er is geen andere rechtsgrond voor de verwerking,
- u bezwaar tegen de verwerking van uw gegevens maakt en er bestaan geen zwaarder doorwegende, gerechtvaardigde gronden voor de verwerking,
- uw gegevens onrechtmatig zijn verwerkt,
- uw gegevens gewist moeten worden om te voldoen aan een wettelijke verplichting,

Procedure bij recht van uitwissing

1. Indienen van een verzoek

In de externe privacyverklaring wordt omschreven op welke manier de Betrokkene een verzoek tot uitwissing kan indienen. Dit gebeurt bij PYRAMID NV door verzending naar een specifiek e-mailadres: gdpr@pauwelsconsulting.com

2. Beslissing over het verzoek

Door de technologische vooruitgang is het hoogst waarschijnlijk dat een recht op vergetelheid niet echt mogelijk gezien de gegevens wellicht ook bij andere verwerkers zijn terechtgekomen. Alle redelijke maatregelen worden genomen om de andere verwerkingsverantwoordelijken die uw gegevens verwerken ervan te verwittigen dat u hebt gevraagd alle links naar uw persoonsgegevens of iedere kopie of reproductie ervan te wissen. Het gaat hier dus niet om een resultaatsverplichting maar eerder om een inspanningsverplichting.

Het verzoek tot uitwissing van gegevens zal geweigerd worden wanneer dit gerechtvaardigd is zoals bijvoorbeeld:

- voor het uitoefenen van het recht op vrijheid van meningsuiting en het recht op informatie;
- voor het naleven van een wet waarvoor het noodzakelijk is dat uw gegevens worden verwerkt of om een opdracht van algemeen belang te vervullen of voor het uitoefenen van het openbaar gezag;
- de verwerking is noodzakelijk om redenen van algemeen belang op het gebied van volksgezondheid;
- de verwerking is noodzakelijk voor wetenschappelijk of historisch onderzoek of voor statistische doeleinden en voor zover het recht op gegevensverwijdering de verwezenlijking van de doeleinden van die verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen;
- De gerechtvaardigde belangen opwegen tegen de belangen van de betrokkene;
- voor de instelling, uitoefening of onderbouwing van een rechtsvordering.

3. Antwoord

Het antwoord en de eventuele uitwissing zal gebeuren zonder onredelijke vertraging.

3) Recht op beperking van de verwerking

De betrokkene heeft het recht om de verwerking van zijn persoonsgegevens te beperken in een aantal gevallen nl:

- Wanneer de betrokkene de juistheid van de persoonsgegevens ter discussie stelt
- Wanneer de betrokkene meent dat de verwerking onrechtmatig is en zich verzet tegen het wissen van de gegevens en in de plaats om beperking van de verwerking verzoekt
- Wanneer de organisatie de gegevens niet langer nodig heeft maar de betrokkene de gegevens nodig heeft voor de instelling, uitoefening, of onderbouwing van een rechtsvordering
- De betrokkene bezwaar maakt tegen de verwerking en in afwachting van de uitkomst van de afweging.

Procedure bij recht op beperking

1. Informatieplicht en ontvangen van een verzoek

In de externe privacyverklaring wordt omschreven op welke manier de Betrokkene een verzoek tot beperking kan indienen. Dit gebeurt bij PYRAMID NV door verzending naar een specifiek e-mailadres met identificatie: gdpr@pauwelsconsulting.com.

2. Onderzoek van het verzoek

Tijdens het onderzoek naar de beperking van de verwerking wordt de verwerking van deze persoonsgegevens zoveel als mogelijk stopgezet.

3. Beslissing over het verzoek

Indien wordt besloten dat het verzoek tot beperking van de betrokkene gerechtvaardigd was, is het niet meer toegestaan om de betreffende persoonsgegevens te verwerken.

Wanneer de Verantwoordelijke voor de verwerking de persoonsgegevens toch verder wenst te verwerken is dit enkel mogelijk in volgende omstandigheden:

- Wanneer de betrokkene opnieuw toestemming geeft;
- Met het oog op een rechtsvordering of ter bescherming van de rechten van anderen
- Bij dringende reden van algemeen belang voor de Unie of voor een lidstaat;

4. Kennisgeving

Indien de persoonsgegevens in kwestie werden doorgegeven aan een derde, geeft PYRAMID NV de ontvangers informatie over het recht tot beperking waarom de betrokkene heeft verzocht, tenzij dit onmogelijk blijkt of onevenredig veel inspanning vergt.

De onderneming antwoordt binnen een redelijke termijn van maximum 1 maand, eventueel verlengd bij complexere zaken.

4) Een betrokkene kan bezwaar maken tegen de verwerking

Een betrokkene heeft het recht om bezwaar te maken tegen de verwerking van zijn persoonsgegevens, met inbegrip van profilering op basis van die bepalingen.

Procedure bij het recht op bezwaar van de betrokkene

1. Indienen van het verzoek

In de externe privacyverklaring wordt omschreven op welke manier de Betrokkene een verzoek tot beperking kan indienen. Dit gebeurt bij PYRAMID NV door verzending naar een specifiek e-mailadres met identificatie: gdpr@pauwelsconsulting.com.

2. Beslissing over het verzoek

Indien de betrokkene bezwaar maakt tegen het verwerken van zijn persoonsgegevens voor direct marketing doeleinden (m.i.v. profiling), dient de verantwoordelijke voor de verwerking hier gehoor aan te geven.

Indien de betrokkene bezwaar maakt tegen de verwerking op basis van algemeen belang en gerechtvaardigd belang, zal de Verantwoordelijke voor de verwerking de verwerking moeten staken tenzij hij:

- dwingende gerechtvaardigde gronden voor de verwerking aanvoert die zwaarder wegen dan de belangen, rechten en vrijheden van de betrokkene, of;
- deze nodig heeft voor de instelling, uitoefening of onderbouwing van een rechtsvordering.

Deze al dan niet verdere verwerking moet dus wel gemotiveerd worden. Het indienen van bezwaar is kosteloos.

3. Het antwoord

De beslissing wordt binnen een redelijke termijn van 1 maand, eventueel verlengde termijn, genomen die nodig is voor PYRAMID NV om het bezwaar te onderzoeken.

5) Overdraagbaarheid van de gegevens;

Een betrokkene mag voor alle verwerkingen van persoonsgegevens die gebaseerd zijn op uitdrukkelijke toestemming of de uitoefeningen van de arbeidsovereenkomst de werkgever vragen om deze te verkrijgen in een gestructureerde gangbare en machine-leesbare vorm.

Het toepassingsgebied van dit recht is ook beperkt aangezien de betrokkene alleen de gegevens zal ontvangen die hij zelf heeft verstrekt.

In de andere gevallen kan de betrokkene dus niet van dat recht genieten, bijvoorbeeld wanneer de verwerking van de gegevens gebeurt op basis van een wet.

Procedure voor recht tot overdraagbaarheid van de gegevens

1. Indienen van een verzoek en beslissing

Indien de Betrokkene hierom verzoekt, is de onderneming gehouden om deze persoonsgegevens (in een gangbare en machine leesbare vorm) rechtstreeks aan een andere organisatie over te maken.

Bij weigering dient u deze beslissing te motivering.

2. Termijn

U dient een dergelijke vraag van een Betrokkene zonder onredelijke vertraging tenzij de vraag complexe zaken met zich meebrengt, waarvan de betrokkene op de hoogte wordt gesteld.

III.VI Procedure bij datalekken

1) Identificatie van een datalek

Een datalek (of een vermoeden ervan) kan op verschillende wijzen worden geïdentificeerd: automatisch door computersystemen, door een werknemer binnen de eigen onderneming of door melding van buitenaf.

Van zodra iemand binnen de onderneming kennis heeft van een datalek maakt deze hiervan onmiddellijk melding bij de DPO of in geval geen DPO is aangesteld de bevoegde persoon voor privacygegevens binnen de onderneming (voor de duidelijkheid wordt de term DPO hierna steeds gehanteerd).

De melding houdt volgende informatie in – voor zover deze onmiddellijk te achterhalen valt:

- de aard van het datalek:

  - verlies of beschadiging van data,
  - vermindering of wegvallen van toegankelijkheid, en/of
  - inbreuk op de vertrouwelijkheid van data;
- de identificatie van data;
- de impact op de organisatie; en
- de vermoede oorzaak.

Melding van datalekken dient te gebeuren bij ontdekking ervan. Eenieder die datalekken opmerkt, houdt zich ter beschikking van de DPO voor verdere opvolging.

2) Analyse door DPO

Bij ontvangst van meldingen van datalekken, zal de DPO steeds onmiddellijk overgaan tot een eerste analyse.

1. Indien er geen sprake is van een datalek, of er zijn geen persoonsgegevens betrokken, of het datalek houdt geen risico's in op de rechten en vrijheden van de betrokkenen, rapporteert de Functionaris aan het Management Team en gaat over naar Punt 10.

2. Indien er sprake is van een datalek met persoonsgegevens die vermoedelijk een risico inhoudt op de rechten en vrijheden van één of meerdere betrokkenen, en het datalek is beperkt in omvang en impact en geen van onderstaande vereisten zijn voldaan, gaat de Functionaris zelf over tot afhandeling van het incident, rapporteert aan het Management Team en gaat over naar Punt 4.

3. Indien er sprake van een datalek met persoonsgegevens die vermoedelijk een risico inhoudt op de rechten en vrijheden van één of meerdere betrokkenen, en één of meerdere van volgende vereisten zijn voldaan:

- er is een vermoeden van impact op de IT-infrastructuur;
- er is een vermoeden van kwaadwillig opzet;
- er is een vermoeden van impact op gevoelige gegevens;
- er is een vermoeden van impact op een grote set van data;

- er is een vermoeden van impact op data van een groot aantal betrokkenen;
- iedere andere situatie die ernstig genoeg is om het Crisis Team mee te betrekken in de evaluatie;

roept de DPO onverwijld het Crisis Team samen en gaat over naar punt 3.

3) Samenroepen Crisis Team

Indien noodzakelijk zal de DPO de bevoegden samenroepen.

Indien een persoon binnen de organisatie wordt opgeroepen, maar niet aanwezig kan zijn, wordt een vervanger aangeduid. Van zodra het Crisis Team wordt samengeroepen, komt deze onmiddellijk samen en analyseert het incident. Ieder lid van het Crisis Team draagt vanuit zijn/haar functie, kennis en expertise bij tot de analyse van het incident.

Indien het Crisis Team merkt dat bepaalde expertise afwezig is en externe bijstand zou nodig zijn, wordt hier melding van gemaakt en wordt gezocht naar een extern adviseur.

Van iedere meeting wordt een verslag opgemaakt met volgende gegevens:

- aanwezigheden (niet verplicht fysiek)
- plaats en tijdstip van begin en einde
- rapportering van de werknemer die het datalek gemeld heeft en van de DPO (eerste meeting), dit kan ook anoniem gebeuren.
- rapportering van werkpunten uit vorige meetings
- nauwkeurige weergave van wat besproken werd
- beslissingen die genomen werden
- communicatiemaatregelen
- frequentie en aantal meetings (eerste meeting)
- eventueel een stappenplan met actiepunten en agendering van een vervolgmeeting

4) Evaluatie

Zowel de DPO individueel als het Crisis Team gaan over tot analyse van het datalek en onderzoeken:

- de aard van het datalek
- de categorieën en aantal betrokkenen in het incident
- de categorieën en aantal gegevens in het incident
- de impact op de onderneming
- een inschatting van de impact op de rechten en vrijheden van de betrokkenen
- eventuele gevolgen van het incident
- maatregelen die het datalek moeten verhelpen en de gevolgen van het datalek moeten vermijden of verminderen
- maatregelen die toekomstige incidenten kunnen vermijden

5) Melding aan privacy autoriteiten

De meldingsplicht geldt niet voor elk beveiligingsincident - d.w.z. een "inbreuk (in de zin van incident) in verband met persoonsgegevens" zoals gedefinieerd in artikel 4.12 AVG, maar enkel voor deze die een risico inhouden voor de rechten en vrijheden van natuurlijke personen (artikel 33 AVG).

Een beveiligingsincident is 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 persoonsgegevens.

Het gaat bijvoorbeeld om beveiligingsincidenten die een impact hebben op de beschikbaarheid, integriteit of vertrouwelijkheid van persoonsgegevens (art. 32 AVG).

Indien de DPO of het Crisis Team een risico detecteren op schending van de rechten en vrijheden van de betrokkene, melden zij dit aan de privacy autoriteiten.

Bij deze melding wordt minstens een opgave gedaan van de wettelijk verplichte informatie ingevolge artikel 33 GDPR:

- de aard van het datalek;
- indien mogelijk, de categorieën en aantal betrokkenen in het incident;
- indien mogelijk, de categorieën en aantal gegevens in het incident;
- de naam en contactgegevens van de Functionaris (of DPO indien deze aangesteld werd)
- eventuele gevolgen van het datalek; en

- maatregelen die het datalek moeten verhelpen en de gevolgen van het datalek moeten vermijden of verminderen.

Er wordt steeds naar gestreefd om meldingen aan de privacy autoriteiten uit te voeren binnen de wettelijke termijn van 72 uur volgend op de ontdekking van het datalek.

Indien het niet mogelijk zou zijn om bepaalde informatie te verzamelen binnen de termijn van 72 uur na ontdekking van het datalek, wordt deze onverwijld verstrekt aan de privacy autoriteiten.

Indien melding wordt gedaan aan de privacy autoriteiten na de termijn van 72 uur, bevat de melding eveneens een verantwoording van de laattijdigheid.

Indien het gedetecteerde risico laag blijft, wordt overgegaan naar Punt 8.

6) Melding aan betrokkenen

Indien de Functionaris of het Crisis Team een hoog risico detecteren op schending van de rechten en vrijheden van de betrokkene, melden zij dit aan de betrokkenen in een duidelijke en heldere taal.

Minstens wordt volgende informatie verstrekt:

- de naam en contactgegevens van de DPO
- eventuele gevolgen van het datalek; en
- maatregelen die het datalek moeten verhelpen en de gevolgen van het datalek moeten vermijden of verminderen.

De melding aan betrokkenen is niet noodzakelijk indien:

- technische en organisatorische maatregelen werden genomen, zoals encryptie, die de gegevens onleesbaar hebben gemaakt;
- maatregelen werden genomen naar aanleiding van het datalek die ieder risico op schending van de privacy uitsluiten; of
- dergelijke melding niet mogelijk is, en een vervangende publieke mededeling wordt gedaan.

7) Openbaarmaking

Indien een melding aan de betrokkene wettelijk verplicht is, doch onredelijk hoge inspanningen en investeringen zou vereisen, dient een publieke mededeling te worden gedaan. Het Crisis Team kan ook beslissen dat een publieke mededeling wenselijk is.

Alleszins moet er steeds over gewaakt worden dat iedere publieke mededeling:

- geen onnodige angst of paniek veroorzaakt;
- beperkt is tot feiten en deze steeds zijn afgetoetst binnen het Crisis Team;
- aangeeft dat de nodige maatregelen worden genomen;
- geen melding doet van persoonsgegevens zelf; en
- contactgegevens meedeelt waar meer informatie kan worden bekomen.

Enkel de Managing Director is bevoegd deze publieke mededelingen uit te voeren.

8) Herstelmaatregelen en uitvoeren actieplan

De DPO en het Crisis Team sturen binnen de organisatie de juiste personen en diensten, en indien nodig de externe dienstverleners, aan om het vooropgestelde actieplan uit te voeren en de beoogde maatregelen te implementeren. De mogelijke oorzaken van het incident worden ingedijkt, defecten worden hersteld, mogelijke infecties worden verwijderd en de systemen worden hersteld in hun oorspronkelijke toestand van voor het incident.

De DPO zal toezien op de correcte uitvoering van het actieplan en verzorgt de verdere opvolging.

Van de uitvoering van het actieplan en de implementatie van de maatregelen wordt een gedetailleerd verslag bijgehouden.

Iedere persoon die betrokken wordt bij de uitvoering van het actieplan en/of de implementatie van de maatregelen rapporteert op geregelde tijdstippen aan de DPO.

- Einde van het incident

  Op basis van de rapporteringen en de besprekingen op de meetings van het Crisis Team, kan de DPO vaststellen dat het incident kan worden afgesloten.

  Een incident kan worden afgesloten indien:

- de situatie onder controle is (of binnen aanvaardbare proporties is herleid);
- de geïmplementeerde maatregelen het gewenste effect bereiken;
- er geen risico op schending van rechten en vrijheden van betrokkene meer bestaat; én
- aan wettelijke verplichtingen tijdig werd voldaan.

Bij beëindiging van het incident wordt het Crisis Team ontbonden en wordt intern gecommuniceerd dat het incident gesloten is.

Indien de situatie onder controle is dankzij tijdelijke maatregelen, maar een definitieve maatregel noodzakelijk is voor het afsluiten van het incident, kan de Functionaris beslissen om het incident onder voorbehoud van implementatie van de definitieve maatregel af te sluiten.

- Rapportering

Elk incident moet worden geregistreerd. Bij hoog risico maakt de DPO een rapport op over het datalek waarin alle relevante documenten, communicatie en verslagen worden opgenomen en die een weergave biedt van de aard van het datalek, de wijze waarop gehandeld is, de genomen maatregelen, de betrokken personen, een vervolgrapport en de aanbevelingen naar de toekomst.

- Aanvullen Register

De DPO vult het overzicht van datalekken in een Register aan en vermeldt minstens:

- de aard van het datalek en de feitelijke omstandigheden;
- de effecten van het datalek op de organisatie en op de rechten en vrijheden van de betrokkenen;
- de genomen maatregelen; en
- eventuele aanbevelingen naar de toekomst.

IV. Hoofdrolspelers met betrekking tot de Verwerking Persoonsgegevens

De Managing Director

De Managing Director is eindverantwoordelijke voor het algemeen beheer van de organisatie.

Het intern privacybeleid is een belangrijk onderdeel van het algemeen beheer van de organisatie. De Managing Director bepaalt de strategische richtlijnen, maar delegeert de operationele verantwoordelijkheid voor fysieke beveiliging en informatiebeveiliging naar de Data Protection Officer.

De Managing Director ondersteunt het engagement naar beveiliging van persoonsgegevens door

Het managementteam

Het management van elke afdeling is verantwoordelijk voor het op een behoorlijke manier verwerken van de Persoonsgegevens van hun afdeling.

Managers

Het is de verantwoordelijkheid van alle managers

- erop toe te zien dat alle medewerkers en contractanten het privacybeleid kennen, begrijpen en naleven
- informatie te verzamelen over de effectiviteit van beveiligingsmaatregelen en deze te rapporteren aan de Data Protection Officer
- de Data Protection Officer te informeren over elke werkelijke en mogelijke schending van het privacybeleid m.b.t. tot de middelen waar zij verantwoordelijk voor zijn

Information Asset Owners

Information Asset Owners zijn verantwoordelijk voor de beveiliging van de hun toegewezen bedrijfsmiddelen. Ze kunnen taken delegeren, maar blijven wel de eindverantwoordelijke voor

- De classificatie van de bedrijfsmiddelen
- Het opzetten van specifieke controlemiddelen
- Toegang verlenen tot de bedrijfsmiddelen, in overeenstemming met de classificatie

- Deelnemen aan of organiseren van security risk assessments om erop toe te zien dat veiligheidsvereisten correct gedefinieerd zijn en bedrijfsmiddelen voldoende beschermd zijn

Een Information Asset Owner kan voor een bedrijfsmiddel een tijdelijke vrijstelling van het voldoen aan de beveiligingsvereisten of verzachtende omstandigheden vragen aan de Data Protection Officer. De Data Protection Officer zal de tijdelijke vrijstelling beoordelen en afhankelijk van het risico aanvaarden of afkeuren. De Information Asset Owner is wel verantwoordelijk voor het opstellen van een actieplan om na verloop van tijd toch te kunnen voldoen aan de beveiligingsvereisten.

De Data Protection Officer (hierna DPO)

Advocaat Jents Debruyne wordt aangesteld als Data Protection Officer van PYRAMID NV

De 'Functionaris Gegevensbescherming' of 'Data Protection Officer' (Hierna DPO) staat in voor het toezicht op en de naleving van de 'Algemene Verordening Gegevensbescherming'. De DPO kan gezien worden als de preventie-adviseur bij uitstek voor verwerkingen van persoonsgegevens. De taken van de DPO zijn de volgende:

- De DPO houdt toezicht op de nieuwe wetgeving en haar verplichtingen. Dit behelst onder meer het bijhouden van een register inzake de verwerking van persoonsgegevens. Ook wordt verwacht dat de DPO voldoende informatie en advies geeft over dit thema aan de verschillende belanghebbenden.

- De DPO beheert het beleid rond de verwerking van persoonsgegevens en stelt een plan op om dit te implementeren en op te volgen. Verder worden overeenkomsten (Bv. contracten met derden) aangevuld en de nodige documenten opgemaakt. Indien reeds een beleidsplan bestaat wordt het bestaande aangevuld zodat aan de verplichtingen van de Algemene Verordening Gegevensbescherming wordt voldaan.
- De DPO volgt interne controles op bij de verwerking van persoonsgegevens en schat daarbij de risico's van een inbreuk op de rechten van personen in. Bij een hoog risico wordt een 'Gegevensbeschermingseffectenbeoordeling' of 'Privacy Impact Assessment' (hierna PIA) opgesteld. Vanuit deze beoordeling adviseert de DPO verbeteringsacties en volgt de status ervan op.

- De DPO volgt de specifieke procedures aangaande datalekken op.
- De DPO werkt mee aan de bewustmaking van de medewerkers voor dit thema.
- De DPO volgt evoluties op inzake wetgeving rond de rechten van de betrokkenen. In overleg met de betrokken IT-diensten worden de mogelijkheden bekeken om deze rechten toe te passen in de IT-systemen.
- De DPO is een aanspreekpunt voor de toezichthoudende Autoriteit. Dit is op heden de 'Belgische Privacycommissie'. Er ligt een wetsontwerp klaar waarin de Privacycommissie wordt omgevormd tot de 'Belgische Gegevensbeschermingsautoriteit'.

De DPO dient onafhankelijk te zijn. Met onafhankelijkheid wordt bedoeld dat de DPO niet de middelen en het doel van de verwerking van persoonsgegevens waarover hij advies geeft mag bepalen. Iemand uit het managementteam kan dus niet fungeren als DPO.

Medewerkers, Zelfstandige dienstverlening, Interim-Overeenkomsten

Medewerkers en contractanten zijn verantwoordelijk voor

- het voldoen aan de beveiligingsvereisten en procedures die relevant zijn voor hun taken, het waarborgen van de opvolging van dit beleid en de bijkomende reglementen in het bijzonder het beleid 'Veilig personeel';
- de beveiliging van de aan hen toevertrouwde informatie.

V. Beschermingsmaatregelen

In het volgende hoofdstuk worden de beveiligingsmaatregelen besproken die worden opgenomen in het intern Privacybeleid. Deze zorgen ervoor dat de persoonsgegevens en in het bijzonder de zogenaamde bijzondere categorieën van persoonsgegevens op een passende wijze zoveel als mogelijk worden beveiligd.

Het intern Privacybeleid wordt ondersteund door volgende procedures:

- Beleidsdocumenten: Veilig Personeel, beleid Personeelsgegevens, Privacy Impact Assessment;
- Beheer van bedrijfsmiddelen & opslagplaatsen;
- Technische beveiliging (cryptografie);
- Toegangsbeveiliging;
- Fysieke beveiliging;
- Beveiliging van bedrijfsvoering;
- Communicatiebeveiliging;
- Procedure datalekken;
- E-Mail beleid;
- Beleid omtrent Direct Marketing, toestemming bekomen en bewaren van gegevens.

Beleidsdocumenten

De beleidsdocumenten en aanbevelingen van de IT-manager dienen opgevolgd te worden zodoende dat de technische beveiliging in de mate van het mogelijke kan gebeuren.

Audit op regelmatige basis door Data Protection Officer minstens binnen 2 jaar wordt alles opnieuw geëvalueerd;

Er worden voldoende passende en technische maatregelen getroffen;

Vertrouwelijkheids- of geheimhoudingsovereenkomst
Een clausule van geheimhouding wordt toegevoegd aan het beleid. Ook met derden wordt een clausule met betrekking tot de waarborgen van de GDPR i.v.m. Persoonsgegevens geïmplementeerd. Indien de standaard clausule van geheimhouding niet afdoende is voor de klant, kan in onderling overleg, een toevoeging daarop gemaakt worden.

Beheer van bedrijfsmiddelen

1. Netwerkapparatuur

Een wijziging aan netwerkapparatuur wordt beschouwd als een significante wijziging en moet door de IT-manager voldoende en uitgebreid worden getest vooraleer deze wordt geïmplementeerd.

Netwerkapparatuur moet worden beheerd met behulp van de beheertools van de leverancier.

2. Mobiele apparatuur

Zie het beleid omtrent mobiele apparatuur zoals bijgevoegd.

3. Wachtwoordpolicy

Het gebruik van complexe wachtwoorden wordt aanbevolen. Een sterk wachtwoordbeleid stelt volgende eisen aan de wachtwoorden:

- Het wachtwoord mag geen deel van de (voor)naam van de gebruiker bevatten.
- Het wachtwoord moet minimaal 8 karakters lang zijn.
- Het wachtwoord moet voldoen aan 3 van de 4 volgende voorwaarden:
    - Hoofdletters
    - Kleine letters
    - Cijfers (0 – 9)
    - Speciale karakters (bijvoorbeeld: !, $, #, @, %)

Op uw apparaat mag geen mapje/document aanwezig zijn waarin u uw wachtwoord opslaat. De wachtwoorden worden gewijzigd om de 6 maanden.

4. Technische aspecten

In verband met de technische aspecten van beveiligingsmaatregelen worden de instructies van de IT-manager nauwgezet opgevolgd.

PYRAMID NV levert inspanningen zoveel als mogelijk volledige informatieveiligheid na te streven. Zij werkt hiervoor samen met kwalitatieve leveranciers;

Volgende IT –beveiligingsmaatregelen worden regelmatig geüpdatet:

4 BESCHERMINGSMATRIX

Afhangend van uw type onderhoudscontract, zijn volgende punten voor u van toepassing:

Item	Maatregel	Geactiveerd in uw omgeving
2.1	Firewall	☒
2.2	Monitoring	☒
2.3	Updates	☒
2.4	Antivirus	☒
2.5	Managed Backup	☒srv-gt-dmn, srvsql, srvrdsnew, srv-bxl-dmn
2.5	Local Speedvault	☒
2.5	Backup van laptops	☐
2.6	Office 365	☒
2.6	Office Advanced Threat Protection	☒
3.1	Wachtwoordbeleid: complexiteit	☒
3.1	Wachtwoorden verlopen.	☒
3.2	Beveiliging externe toegang via VPN	☒
3.2	Beveiliging externe toegang remote desktop	☒
3.3	Encryptie Harde Schijven (Bitlocker)	☒
3.4	Werkposten vergrendelen	☒

Verder tracht PYRAMID NV zoveel als mogelijk te werken volgens het principe van privacy by design en de instructies van Business solutions op te volgen.

5. Fysieke beveiliging; Toegangsbeveiliging

Het kantoor wordt beveiligd door deuren en aanmelding bij de receptie. Medewerkers hebben persoonlijke badge & sleutel.

De server wordt in een afgezonderd lokaal geplaatst met voldoende afkoelingsmogelijkheden.

Toegangsrechten met betrekking tot het netwerk worden voldoende gesegmenteerd. Deze worden aangepast per afdeling / bij gevoelige informatie hebben slechts enkele mensen toegang tot deze gegevens.

6. Communicatiebeveiliging

Bij de communicatie met externe partijen dient telkens te worden nagegaan of het gekozen communicatiemiddel volstaat voor het soort informatie dat moet worden verstuurd, rekening houdend met de classificatie van het bedrijfsmiddel. Tevens moeten steeds de persoonsgegevens zoveel als mogelijk worden afgeschermd.

7. Beleid voor mobiele apparatuur

Doelstelling

De doelstelling van het beleid voor mobiele apparatuur en telewerken is:

- Bepalen welke mobiele apparatuur gebruikt mag worden
- Beschrijven hoe moet omgegaan worden met mobiele apparatuur
- Waarborgen van de veiligheid bij gebruik van mobiele apparatuur
- Beschrijven welke vormen van telewerken toegelaten zijn
- Waarborgen van de veiligheid van telewerken

8. Beleid voor informaticamateriaal

PYRAMID NV stelt divers informaticamateriaal individueel ter beschikking van haar medewerkers /contractanten, zodat zij in staat zijn hun job efficiënt uit te voeren. Dit toevertrouwd ICT-materiaal kan onder andere bestaan uit:

- Portable computer met accessoires (draagtas, power supplies, muis, en dergelijke)
- Smartphone
- Tablet
- Harde schijf
- USB
- Authenticatie token om vanop afstand te kunnen werken
- …

Mobiele apparatuur, die eigendom is van PYRAMID NV moet door de medewerkers en contractanten fysiek beschermd worden. Mobiele apparatuur:

- mag niet onbeheerd achtergelaten worden. Indien een toestel toch korte tijd onbeheerd achtergelaten wordt, dan moet het toestel gelocked worden, beveiligd

met een paswoord. Het systeem zal een toestel automatisch locken na ten langste 10 minuten inactiviteit.

- mag 's nachts niet onbeschermd op een bureau blijven staan, maar moet in de afgesloten locker opgeborgen worden, of meegenomen worden naar huis
- moet in de afgesloten kofferruimte van de auto geplaatst worden
- mag 's nachts niet achtergelaten worden in een auto die niet in een garage staat (ook niet als de apparatuur in de kofferruimte zit)
- mag niet door derden gebruikt worden
- dient enkel voor professioneel gebruik
- mag niet gebruikt worden om professionele informatie op te slaan, die niet ook beschikbaar is op de servers van PYRAMID NV (de lokale harde schijf van de mobiele apparatuur wordt niet geback-upt)
- is beschermd met een persoonlijke loginnaam en paswoord. Het paswoord is strikt persoonlijk en mag met niemand gedeeld worden binnen of buiten PYRAMID NV. Het systeem verplicht de medewerker om dit paswoord voldoende complex te maken en op regelmatige tijdstippen te wijzigen.

De software, patches, beveiliging en antivirussoftware op deze toestellen worden regelmatig up-to-date gehouden. Installatie van bijkomende software op een portable computer vereist goedkeuring van de IT-manager. Bij voorkeur wordt te installeren software ter beschikking gesteld.

Medewerkers en contractanten mogen voor hun professionele taken gebruik maken van hun eigen smartphone of tablet, mits deze beveiligd zijn met een Pincode of biometrische gegevens.

De mobiele apparaten worden als een goede huisvader onderhouden door de gebruiker.

Elke gebruiker is zelf verantwoordelijk voor het instellen, het beheren en de beveiliging van de eigen apparaten die men gebruikt. De Gebruikers zijn aansprakelijk voor elk gebruik of misbruik van dit gebruiksrecht. Om veiligheidsredenen kunnen bepaalde diensten en websites geblokkeerd worden. De gebruiker mag het apparaat niet op een ongeoorloofde manier gebruiken of aanwenden voor onwettige doeleinden/illegale zaken, zoals het lastigvallen van anderen, het verspreiden van smadelijke of discriminerende teksten of het schenden van auteursrechten.

Beschermingsmaatregelen

De informatie die op deze mobiele apparaten staat dient bij beëindiging van het gebruik van dit apparaat zorgvuldig worden gearchiveerd en daarna verwijdert. Bij hergebruik van de apparatuur worden zij eerst onderzocht door de IT-manager die de veiligheid en werking van het apparaat zal beoordelen op functionaliteit en veiligheid.

Tot slot: Wanneer een werknemer of enig ander persoon een vermoeden heeft van een beveiligingstekort kan deze dit melden aan de DPO/bevoegde persoon.

VI. Opvolging

1. Interne bekendmaking

De privacy beleidsdocumenten worden intern ter beschikking gesteld op het intranet van Pyramid NV en Pauwels Consulting.

2. Evaluatiemomenten

Jaarlijks worden de volgende zaken geëvalueerd:

- Is het beleid nog op punt met betrekking tot de persoonsgegevens;
- Zijn de beveiligingsmaatregelen nog actueel;
- Welke Privacy Impact Assessments zijn er gebeurd;
- Welke beveiligingsincidenten/datalekken hebben zich voorgedaan;
- Dienen bijkomende maatregelen worden getroffen;

Een rapport wordt opgesteld binnen PYRAMID NV door de DPO.

3. Contact

DPO/ Bevoegde persoon: jents@advocaatdebruyne.be - 0479/50.46.35

Bedrijfsgegevens

PYRAMID NV

Lambroekstraat 5A

1831 Diegem

Tel +32 9 324 70 80

www.pauwelsconsulting.com