Protocol AVG Buro Noorderlingen

1. Inleiding

Dit protocol beschrijft het beleid dat door Buro Noorderlingen wordt gevoerd in het kader van de Algemene verordening gegevensbescherming (AVG). De verordening regelt de privacy rechten voor burgers en de verantwoordelijkheden van organisaties in het beschermen hiervan.

In paragraaf twee worden de kaders ten behoeve van het gegevensbeschermingsbeleid uiteengezet. Vervolgens worden op basis van deze kaders in paragraaf drie de concrete afspraken geformuleerd over de wijze waarop met gegevensverwerking en gegevensdragers wordt omgegaan. Paragraaf vier gaat tenslotte in op de verplichte registers die moeten worden bijgehouden in het kader van dit protocol.

2. Gegevensbeschermingsbeleid

Uitgangspunt van het gegevensbeschermingsbeleid is een algemeen bewustzijn binnen de organisatie van de gegevens die worden verwerkt, wat het doel, de omvang en de context daarvan zijn. Vastleggen moet een doel dienen en er moet bewustzijn bestaan over wat de impact is wanneer gegevens onbedoeld gedeeld worden met niet-belanghebbenden. Dit vraagt om zorgvuldigheid van alle betrokkenen in de organisatie.

In algemene zin vindt verwerking van persoonsgegevens uitsluitend plaats in relatie tot het doel van de trajecten. Hierbij wordt voldaan aan wettelijke eisen met betrekking tot het vastleggen van gegevens, maar wordt nooit meer gedaan dan wettelijk op dit gebied is voorgeschreven. De betrokken personen en organisaties zijn op de hoogte van het vastleggen van de gegevens. Deze zijn uitsluitend voor intern gebruik gedurende de duur van een traject. Indien gegevens extern gecommuniceerd wordt gaat dit te allen tijde in overleg met alle betrokkenen

2.1 Borgen van rechten van betrokkenen

Betrokkenen hebben het recht op inzage, correctie en dataportabiliteit van persoonsgegevens.

- Recht op **inzage** in de persoonsgegevens

  Indien een betrokkene hierom vraagt, biedt Buro Noorderlingen inzage in de persoonsgegevens die zijn vastgelegd.

- Recht op **correctie en verwijdering** van persoonsgegevens

  Een betrokkene kan om correctie of verwijdering van persoonsgegevens vragen als deze feitelijk onjuist zijn, onvolledig zijn of niet ter zake doen voor het doel waarvoor ze zijn

verzameld of op een andere manier in strijd met een wet worden gebruikt. Het correctierecht is niet bedoeld voor het corrigeren van professionele indrukken, meningen en conclusies waarmee iemand het niet eens is, voor zover deze ter zake doen.

- Recht op **dataportabiliteit**
  De (digitale) persoonsgegevens die Buro Noorderlingen verwerkt (met toestemming van betrokkene of om overeenkomst met betrokkene uit te voeren), kunnen op diens verzoek verstrekt worden aan een betrokkene. De vorm waarin de organisatie de gegevens verstrekt moet zodanig zijn dat het voor betrokkene gemakkelijk wordt gemaakt om deze gegevens te hergebruiken en door te geven aan een andere organisatie.

2.2 Schriftelijke toestemming betrokkenen voor gegevensverwerking

Aan betrokkenen wordt altijd expliciet en schriftelijk toestemming gevraagd voor het verwerken van persoonsgegevens. Het moet daarbij voor betrokkenen net zo eenvoudig zijn om hun toestemming in te trekken als om die te geven.

Als randvoorwaarden voor deze toestemming geldt dat betrokkenen:

- Geïnformeerd zijn waarover hij toestemming geeft en dat aangetoond kan worden op basis van welke informatie toestemming is gegeven.
- Specifiek toestemming hebben gegeven voor de gegevens die worden verwerkt.

Indien betrokkenen:

- cliënten zijn, dan is deze toestemming vastgelegd in de coachingsvoorstel of een afspraak per mail.
- medewerkers zijn, dan is deze toestemming vastgelegd in de arbeidsovereenkomst

2.3 Functionaris voor de gegevensverwerking

De functionaris voor de gegevensverwerking (FG) houdt toezicht op de toepassing en naleving van de AVG volgens dit protocol. Dit betekent onder andere het verzamelen van informatie over verwerkingen, analyseren en controleren aan de hand van dit protocol en adviseren aan de verantwoordelijke.

Bij Buro Noorderlingen is deze taak belegd bij de kwaliteitsfunctionaris (Bert Nieuwenhuis), hetgeen concreet inhoudt:

- Betrokkenheid bij de implementatie en toepassing van dit protocol
- Minimaal jaarlijks een audit van (een of enkele van) de processen om naleving te toetsen
- Gevraagd en ongevraagd adviseren over de toepassing van dit protocol

Naast de FG zijn alle medewerkers persoonlijk verantwoordelijk voor het houden van toezicht op de toepassing en naleving van de AVG volgens dit protocol. Dit betekent dat ook zij gevraagd en ongevraagd adviseren over de toepassing hiervan en elkaar en anderen binnen de organisatie actief aanspreken indien buiten de kaders van dit protocol wordt gehandeld.

2.4 Meldplicht datalekken

Er is sprake van een datalek indien als gevolg van een beveiligingsincident persoonsgegevens verloren zijn gegaan of als onrechtmatige verwerking van persoonsgegevens niet uit te sluiten is. Een voorbeeld hiervan is het kwijtraken van een USB-stick of diefstal van een telefoon/laptop.

Buro Noorderlingen doet melding van een datalek bij de Autoriteit Persoonsgegevens indien sprake is van de volgende situaties:

- De gelekte persoonsgegevens zijn van gevoelige aard: bijvoorbeeld de gezondheid of financiële situatie van de betrokkene
- Er is een (grote) kans is op ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens: bijvoorbeeld identiteitsfraude bij het lekken van een kopie van het identiteitsbewijs
- Er sprake is van een grote hoeveelheid gelekte persoonsgegevens, zowel per persoon of met betrekking tot het aantal betrokkenen

De melding wordt binnen 72 uur na de ontdekking van het datalek door Buro Noorderlingen gedaan via de website van de Autoriteit Persoonsgegevens. Bij het lekken van persoonsgegevens van gevoelige aard, meldt Buro Noorderlingen dit altijd aan de betrokkene. De melding stelt de betrokkene in staat om alert te zijn op mogelijke gevolgen van het datalek en daarop te anticiperen.

3. Afspraken gegevensverwerking

De meldplicht voor datalekken, zoals in de voorgaande paragraaf is beschreven, is in beginsel van toepassing op de afspraken voor gegevensverwerking die in deze paragraaf worden benoemd. In onderstaand schema worden de middelen beschreven waarmee gegevens verwerking plaats mag vinden of waarmee gegevens getransporteerd mogen worden. Niet beschreven middelen zijn niet toegestaan te gebruiken. Per middel wordt aangegeven welke minimale eisen aan het gebruik gesteld worden.

Middel	Gebruik
USB-sticks	Uitsluitend te gebruiken binnen Buro Noorderlingen. De USB stick dient met een code beveiligd te zijn en wordt in een afgesloten ruimte bewaard.
Mobiele telefoon	Gebruik uitsluitend persoonsgebonden en op basis van een gebruiksovereenkomst. Telefoon dient met een code beveiligd te worden. Beperkt privégebruik is toegestaan.
Tablet / laptop	Apparatuur dient met een code beveiligd te worden. Apparaten dienen in een afgesloten ruimte bewaard te worden en mogen nooit onbeheerd achtergelaten worden.
PC	Apparatuur dient met een code beveiligd te worden. Bij het verlaten van de werkplek dient uitgelogd te worden en de werkplek afgesloten achtergelaten te worden.
Medewerkersdossier (op papier)	Toegang tot deze gegevens is uitsluitend toegestaan aan de uitvoerende professional. Betrokkenen kunnen inzage krijgen via de genoemde functionarissen tot hun eigen dossier. Dossiers worden bewaard in een afsluitbare kast die is opgesteld in een afsluitbare ruimte.
Papieren documenten	Documenten worden bewaard in een afsluitbare kast die is opgesteld in een afsluitbare ruimte. Afdrukken van documenten is uitsluitend toegestaan binnen de beveiligde omgeving van de printapparatuur (‘printen in de box’). Documenten mogen nooit onbeheerd bij de printer worden achtergelaten.
Digitale documenten	Verwerking uitsluitend binnen de digitale, beveiligde omgeving. Deze omgeving is alleen toegankelijk voor daartoe geautoriseerde medewerkers of belanghebbenden.
Facturen (indien daarop persoonsgegevens zijn vermeld)	Verwerking bij voorkeur binnen de digitale, beveiligde omgeving. Indien afdrukken op papier noodzakelijk is, dan geldt hetzelfde als voor papierendocumenten geldt.

E-mail	In principe worden geen persoonsgegevens per e-mail verspreid. Indien het ten behoeve van de uitvoering van werkzaamheden noodzakelijk is om wel persoonsgegevens per e-mail te delen, dan vindt dit uitsluitend plaats tussen functionarissen in de organisatie of met functionarissen buiten de organisaties op basis van een bewerkersovereenkomst. Bij het delen van informatie wordt uitgegaan van minimalisatie, bijvoorbeeld indien mogelijk het gebruik van initialen in plaats van de gehele naam van betrokkene. De organisatie is zich bewust van het risico dat gepaard gaat met het noodzakelijk delen van privacygevoelige informatie, echter dit risico mag er niet toe leiden dat dit de primaire en ondersteunende werkzaamheden onwerkbaar maakt. Dit vereist van alle betrokkenen een grote zorgvuldigheid en het zorgdragen voor een voldoende adequaat beveiligde werkomgeving.
WiFi	Het WiFi netwerk is beveiligd met een wachtwoord.