**VERWERKERSOVEREENKOMST**

**Versie 1.3 – 22 januari 2021**

Deze verwerkersovereenkomst is een bijlage bij de Overeenkomst en de daarbij behorende bijlagen zoals toepasselijke algemene voorwaarden.

**DE ONDERGETEKENDEN:**

**Ondergetekenden:**

1. \_\_\_\_\_\_\_\_\_\_\_\_\_Klant, gevestigd en kantoorhoudende aan het adres \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_<adres> \_\_\_\_\_\_\_\_\_\_\_\_\_\_<postcode> \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_<plaats>, hierna te noemen **“Opdrachtgever”;** en

2. **XAFAX NEDERLAND B.V.,** gevestigd en kantoorhoudende te Alkmaar, aan het adres (1822 BH), Berenkoog 13, hierbij rechtsgeldig vertegenwoordigd door de heer F. Duijzer, Directeur, hierna te noemen **“Data processor”;**

**OVERWEGENDE DAT:**

a) In verband met de ingang van 25 mei 2018 van toepassing zijnde Verordening 2016/679, ook wel de Algemene Verordening Gegevensbescherming (“AVG”) wensen partijen hierbij de onderhavige verwerkingsovereenkomst (“Verwerkersovereenkomst”) zoals bedoeld in artikel 28 AVG te sluiten.

**VERKLAREN ALS VOLGT TE ZIJN OVEREENGEKOMEN:**

**ARTIKEL 1. DEFINITIES**

Onderstaande begrippen hebben in deze verwerkersovereenkomst de volgende betekenis:

* 1. Autoriteit Persoonsgegevens (AP): toezichthoudende autoriteit, zoals omschreven

in artikel 4, sub 21 Avg.

1.2 Avg: de Algemene verordening gegevensbescherming.

1.3 Data Processor: partij die als ICT-leverancier in het kader van de uitvoering van de Overeenkomst als verwerker Persoonsgegevens verwerkt ten behoeve van diens Opdrachtgever.

1.4 Data subject (betrokkene): een geïdentificeerde of identificeerbare natuurlijke persoon.

1.5 Opdrachtgever: partij in wiens opdracht Data Processor persoonsgegevens verwerkt. De Opdrachtgever kan zowel verwerkingsverantwoordelijke (“controller”) zijn als een andere verwerker.

1.6 Overeenkomst: de tussen Opdrachtgever en Data Processor geldende overeenkomst, op basis waarvan de ICT-leverancier diensten en/of producten levert aan Opdrachtgever, waarvan de verwerkersovereenkomst onderdeel vormt.

1.7 Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, zoals omschreven in artikel 4, sub 1 Avg, die Data Processor in het kader van de uitvoering van zijn verplichtingen voortvloeiende uit de Overeenkomst verwerkt.

1.8 Verwerkersovereenkomst: deze Standaardclausules voor verwerkingen, tezamen de verwerkersovereenkomst vormen als bedoeld in artikel 28, lid 3 Avg.

**ARTIKEL 2. ALGEMEEN**

2.1 Deze Standaardclausules voor verwerkingen zijn van toepassing op alle verwerkingen van Persoonsgegevens die Data Processor doet in het kader van de levering van zijn producten en diensten en op alle Overeenkomsten en aanbiedingen. De toepasselijkheid van verwerkersovereenkomsten van Opdrachtgever wordt uitdrukkelijk van de hand gewezen.

2.2 Bijlage 1, Persoonsgegevens en met name bijlage 2, de beveiligingsmaatregelen, kunnen van tijd tot tijd door Data Processor worden aangepast aan veranderende omstandigheden. Data Processor zal Opdrachtgever van significante aanpassingen op de hoogte stellen. Indien Opdrachtgever in redelijkheid niet akkoord kan gaan met de aanpassingen, is Opdrachtgever gerechtigd binnen 30 dagen na kennisgeving van de aanpassingen de verwerkersovereenkomst schriftelijk gemotiveerd op te zeggen.

2.3 Data Processor verwerkt de Persoonsgegevens namens en in opdracht van Opdrachtgever overeenkomstig de met Data Processor overeengekomen schriftelijke instructies van Opdrachtgever.

2.4 Opdrachtgever, dan wel diens klant, is de verwerkingsverantwoordelijke in de zin van de Avg, heeft de zeggenschap over de verwerking van de Persoonsgegevens en heeft het doel van en de middelen voor de verwerking van de Persoonsgegevens vastgesteld.

2.5 Data Processor is verwerker in de zin van de Avg en heeft daarom geen zeggenschap over het doel van en de middelen voor de verwerking van de Persoonsgegevens en neemt derhalve geen beslissingen over onder meer het gebruik van de Persoonsgegevens.

2.6 Data Processor geeft uitvoering aan de Avg zoals neergelegd in deze Standaardclausules voor verwerkingen en de Overeenkomst en handelt conform de Avg. Het is aan Opdrachtgever om op basis van deze informatie te beoordelen of Data Processor afdoende garanties biedt met betrekking tot het toepassen van passende technische en organisatorische maatregelen opdat de verwerking aan de vereisten van de Avg voldoet en de bescherming van de rechten van Data subjects voldoende zijn gewaarborgd.

2.7 Opdrachtgever staat er tegenover Data Processor voor in dat hij conform de Avg handelt, dat hij zijn systemen en infrastructuur te allen tijde adequaat beveiligt en dat de inhoud, het gebruik en/of de verwerking van de Persoonsgegevens niet onrechtmatig zijn en geen inbreuk maken op enig recht van een derde.

2.8 Een aan Opdrachtgever door de AP opgelegde bestuurlijke boete kan niet worden verhaald op Data Processor, tenzij er sprake is van opzet of bewuste roekeloosheid aan de zijde van de bedrijfsleiding van Data Processor.

**ARTIKEL 3. BEVEILIGING**

3.1 Data Processor treft de technische en organisatorische beveiligingsmaatregelen zoals omschreven in bijlage 2. Bij het treffen van de technische en organisatorische beveiligingsmaatregelen heeft Data Processor rekening gehouden met de stand van de techniek, de uitvoeringskosten van de beveiligingsmaatregelen, de aard, omvang en de context van de verwerkingen, de doeleinden en het beoogd gebruik van zijn producten en diensten, de verwerkingsrisico’s en de qua waarschijnlijkheid en ernst uiteenlopende risico’s voor de rechten en vrijheden van Data subjects die hij gezien het beoogd gebruik van zijn producten en diensten mocht verwachten.

3.2 Het product of de dienst van Data Processor is niet ingericht op de verwerking van bijzondere categorieën van Persoonsgegevens of gegevens betreffende strafrechtelijke veroordelingen of strafbare feiten.

3.3 Data Processor streeft ernaar dat de door hem te treffen beveiligingsmaatregelen passend zijn voor het door Data Processor beoogde gebruik van het product of de dienst.

3.4 De omschreven beveiligingsmaatregelen bieden, naar het oordeel van de Opdrachtgever, rekening houdend met de in artikel 3.1 genoemde factoren een op het risico van de verwerking van de door hem gebruikte of verstrekte Persoonsgegevens afgestemd beveiligingsniveau.

3.5 Data Processor kan wijzigingen aanbrengen in de getroffen beveiligingsmaatregelen indien dat naar zijn oordeel noodzakelijk is om een passend beveiligingsniveau te blijven bieden. Data Processor zal belangrijke wijzigingen vastleggen en zal Opdrachtgever waar relevant van die wijzigingen op de hoogte stellen.

3.6 Opdrachtgever kan Data Processor verzoeken nadere beveiligingsmaatregelen te treffen. Data Processor is niet verplicht om op een dergelijk verzoek wijzigingen door te voeren in zijn beveiligingsmaatregelen. Data Processor kan de kosten verband houdende met de op verzoek van Opdrachtgever doorgevoerde wijzigingen in rekening brengen bij Opdrachtgever. Pas nadat de door Opdrachtgever gewenste gewijzigde beveiligingsmaatregelen schriftelijk zijn overeengekomen en ondertekend door Partijen, heeft Data Processor de verplichting deze beveiligingsmaatregelen daadwerkelijk te implementeren.

**ARTIKEL 4. INBREUKEN IN VERBAND MET PERSOONSGEGEVENS**

4.1 Data Processor staat er niet voor in dat de beveiligingsmaatregelen onder alle omstandigheden doeltreffend zijn. Indien Data Processor een inbreuk in verband met Persoonsgegevens (zoals bedoeld in artikel 4 sub 12 Avg) ontdekt, zal hij Opdrachtgever zonder onredelijke vertraging informeren.

4.2 Het is aan de verwerkingsverantwoordelijke (Opdrachtgever, of diens klant) om te beoordelen of de inbreuk in verband met Persoonsgegevens waarover Data Processor heeft geïnformeerd gemeld moet worden aan de AP of Data subject. Het melden van inbreuken in verband met Persoonsgegevens, die op grond van artikel 33 en 34 Avg moeten worden gemeld aan de AP en/of Data subjects, blijft te allen tijde de verantwoordelijkheid van de verwerkingsverantwoordelijke (Opdrachtgever of diens klant). Data Processor is niet verplicht tot het melden van inbreuken in verband met persoonsgegevens aan de AP en/of de Betrokkene.

4.3 Data Processor zal, indien nodig, nadere informatie verstrekken over de inbreuk in verband met Persoonsgegevens en zal zijn medewerking verlenen aan noodzakelijke informatievoorziening aan Opdrachtgever ten behoeve van een melding als bedoeld in artikel 33 en 34 Avg.

4.4 Data Processor kan de redelijke kosten die hij in dit kader maakt in rekening brengen bij Opdrachtgever tegen zijn dan geldende tarieven.

**ARTIKEL 5. GEHEIMHOUDING**

5.1 Data Processor waarborgt dat de personen die onder zijn verantwoordelijkheid Persoonsgegevens verwerken een geheimhoudingsplicht hebben.

5.2 Data Processor is gerechtigd de Persoonsgegevens te verstrekken aan derden, indien en voor zover verstrekking noodzakelijk is ingevolge een rechterlijke uitspraak, een wettelijk voorschrift of op basis van een bevoegd gegeven bevel van een overheidsinstantie.

5.3 Alle door Data Processor aan Opdrachtgever verstrekte toegangs- en/of identificatiecodes, certificaten, informatie omtrent toegangs- en/of wachtwoordenbeleid en alle door Data Processor aan Opdrachtgever verstrekte informatie die invulling geeft aan de technische en organisatorische beveiligingsmaatregelen zijn vertrouwelijk en zullen door Opdrachtgever als zodanig worden behandeld en slechts aan geautoriseerde medewerkers van Opdrachtgever kenbaar worden gemaakt. Opdrachtgever ziet erop toe dat zijn medewerkers de verplichtingen uit dit artikel naleven.

**ARTIKEL 6. LOOPTIJD EN BEËINDIGING**

6.1 Deze verwerkersovereenkomst maakt onderdeel uit van de Overeenkomst en iedere daaruit voortkomende nieuwe of nadere overeenkomst, treedt in werking op het moment van totstandkoming van de Overeenkomst en wordt gesloten voor onbepaalde tijd.

6.2 Deze verwerkersovereenkomst eindigt van rechtswege bij beëindiging van de Overeenkomst of enige nieuwe of nadere overeenkomst tussen partijen.

6.3 Data Processor zal, in geval van einde van de verwerkersovereenkomst, alle onder zich zijnde en van Opdrachtgever ontvangen Persoonsgegevens verwijderen op zodanige wijze dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn (render inaccessable), of, indien overeengekomen, in een machine leesbaar formaat terugbezorgen Opdrachtgever.

6.4 Data Processor kan eventuele kosten die hij maakt in het kader van het in artikel 6.3 gestelde in rekening brengen bij Opdrachtgever.

6.5 Het bepaalde in artikel 6.3 geldt niet indien een wettelijke regeling het geheel of gedeeltelijk verwijderen of terugbezorgen van de Persoonsgegevens door Data Processor belet. In een dergelijk geval zal Data Processor de Persoonsgegevens enkel blijven verwerken voor zover noodzakelijk uit hoofde van zijn wettelijke verplichtingen. Het bepaalde in artikel 6.3 geldt eveneens niet indien Data Processor verwerkingsverantwoordelijke in de zin van de Avg is ten aanzien van de Persoonsgegevens.

**ARTIKEL 7. RECHTEN DATA SUBJECTS, DATA PROTECTION IMPACT ASSESSMENT (DPIA) EN AUDITRECHTEN**

7.1 Data Processor zal, waar mogelijk, zijn medewerking verlenen aan redelijke verzoeken van Opdrachtgever die verband houden met bij Opdrachtgever door Data subjects ingeroepen rechten van Data subjects. Indien Data Processor direct door een Data subject wordt benaderd, zal hij deze waar mogelijk doorverwijzen naar Opdrachtgever.

7.2 Indien Opdrachtgever daartoe verplicht is, zal Data Processor na een daartoe redelijk gegeven verzoek zijn medewerking verlenen aan een gegevensbeschermingseffectbeoordeling (DPIA) of een daarop volgende voorafgaande raadpleging zoals bedoeld in artikel 35 en 36 Avg.

7.3 Data Processor kan de naleving van zijn verplichtingen op grond van de verwerkersovereenkomst aantonen door middel van een geldig Data Pro Certificaat of daaraan ten minste gelijkwaardig certificaat of auditrapport (Third Party Memorandum) van een onafhankelijke, deskundige.

7.4 Data Processor zal op verzoek van Opdrachtgever alle verdere informatie ter beschikking stellen die in redelijkheid nodig is om nakoming van de in deze verwerkersovereenkomst gemaakte afspraken aan te tonen. Indien Opdrachtgever desondanks aanleiding heeft aan te nemen dat de verwerking van Persoonsgegevens niet conform de verwerkersovereenkomst plaatsvindt, dan kan hij maximaal éénmaal per jaar door een onafhankelijke, gecertificeerde, externe deskundige die aantoonbaar ervaring heeft met het soort verwerkingen dat op basis van de Overeenkomst wordt uitgevoerd, op kosten van de Opdrachtgever hiernaar een audit laten uitvoeren. De audit zal beperkt zijn tot het controleren van de naleving van de afspraken met betrekking tot verwerking van de Persoonsgegevens zoals neergelegd in deze Verwerkersovereenkomst. De deskundige zal een geheimhoudingsplicht hebben ten aanzien van hetgeen hij aantreft en zal alleen datgene rapporteren aan Opdrachtgever dat een tekortkoming oplevert in de nakoming van verplichtingen die Data Processor heeft op grond van deze verwerkersovereenkomst. De deskundige zal een afschrift van zijn rapport aan Data Processor verstrekken. Data Processor kan een audit of instructie van de deskundige weigeren indien deze naar zijn mening in strijd is met de Avg of andere wetgeving of een ontoelaatbare inbreuk vormt op de door hem getroffen beveiligingsmaatregelen.

7.5 Partijen zullen zo snel mogelijk in overleg treden over de uitkomsten in het rapport. Partijen zullen de voorgestelde verbetermaatregelen die in het rapport zijn neergelegd opvolgen voor zover dat van hen in redelijkheid kan worden verwacht. Data Processor zal de voorgestelde verbetermaatregelen doorvoeren voor zover deze naar zijn oordeel passend zijn rekening houdend met de verwerkingsrisico’s verbonden aan zijn product of dienst, de stand van de techniek, de uitvoeringskosten, de markt waarin hij opereert, en het beoogd gebruik van het product of de dienst.

7.6 Data Processor heeft het recht om de kosten die hij maakt in het kader van het in dit artikel gestelde in rekening te brengen bij Opdrachtgever.

**ARTIKEL 8. SUBVERWERKERS**

8.1 Opdrachtgever geeft toestemming aan Data Processor om andere subverwerkers in te schakelen ter uitvoering van zijn verplichtingen voortvloeiende uit de Overeenkomst.

8.2 Data Processor zal Opdrachtgever informeren over een wijziging in de door de Data Processor ingeschakelde derde partijen. Opdrachtgever heeft het recht bezwaar te maken tegen voornoemde wijziging door Data Processor. Data Processor draagt ervoor zorg dat de door hem ingeschakelde derde partijen zich aan eenzelfde beveiligingsniveau committeren ten aanzien van de bescherming van de Persoonsgegevens als het beveiligingsniveau waaraan Data Processor jegens Opdrachtgever is gebonden.

**ARTIKEL 9. OVERIG**

Deze Standaardclausules voor verwerkingen vormen een integraal onderdeel van de Overeenkomst. Alle rechten en verplichtingen uit de Overeenkomst, waaronder begrepen de van toepassing zijnde algemene voorwaarden en/of beperkingen van aansprakelijkheid, zijn derhalve ook van toepassing op de verwerkersovereenkomst.

**Voor akkoord:**

Ik ga akkoord met dit document en verklaar ze te hebben ontvangen en gelezen.

Opdrachtgever: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Xafax Nederland B.V.

Naam: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(tekeningsbevoegd) Fokko Duijzer

Functie: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Directeur


Handtekening:

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Bijlage 1 Persoonsgegevens**

**Versie 2.0 - November 2018**

Algemene informatie

Naam product en/of dienst: Xafax NetPay

Link naar leverancier en/of productpagina: [www.xafax.nl](http://www.xafax.nl)

Omschrijving van de Verwerking

Het verwerken van oplaadtransacties en transacties die plaatsvinden bij multifunctionele printers, vending automaten en kassa’s van betrokkenen.

Categorieën en soorten persoonsgegevens

Afhankelijk van de diensten en functionaliteiten die betrokkene gebruikt, kunnen we onder meer de volgende persoonsgegevens verwerken van betrokkene:

1. identificatiegegevens, zoals naam, achternaam, geslacht en geboortedatum;
2. contactinformatie, zoals (e-mail)adres en (mobiel) telefoonnummer;
3. transactiegegevens, zoals bijschrijvingen en afschrijvingen;
4. financiële gegevens, zoals bankrekeningnummer (in geval betrokkene restitutie wil aanvragen);
5. gegevens over online gedrag en voorkeuren, zoals het IP-adres mobiele apparaat of computer en de pagina’s die betrokkene op de website of in de apps van Xafax bezoekt;
6. gegevens die betrokkene deelt met onze contactdiensten, correspondentie met Xafax en support data (telefoon, chatgesprekken en e-mail).

Alle gegevens die door Xafax verwerkt worden zijn van een niet bijzondere aard.

Categorieën betrokkenen

* Studenten/leerlingen
* Ouders/voogd
* Medewerkers
* Gasten

Doeleinden verwerking

We gebruiken de persoonsgegevens van betrokkene voor de volgende doeleinden:

* Om betrokkene toegang te geven tot zijn account, betrokkene de mogelijkheid te bieden om tegoed te kopen, bestelling te verwerken en gebruik te maken van onze functionaliteiten en diensten;
* Het controleren van de account van betrokkene, token/pas of andere informatie die wordt toegevoegd;
* Het verwerken van betaaltransacties, leveren van tokens/passen, beveiligen van het platform en accounts, identificatiedoeleinden en serviceverlening;
* Het handhaven van de gebruikersvoorwaarden van (my)NetPay;
* Het voldoen aan wet- en regelgeving;
* Het bijstaan van derden bij het verstrekken van producten/diensten die betrokkene bij derden aanvraagt;
* Het oplossen van geschillen en betwiste betaaltransacties;
* Het herkennen, voorkomen, beperken en bestrijden van misbruik en fraude;
* Om contact met betrokkene te onderhouden, betrokkene van informatie te voorzien en vragen, verzoeken of klachten af te handelen;
* Het verkrijgen van inzicht in het gebruik van onze producten en diensten door gegevensanalyses te verrichten ter verbetering daarvan.

Bewaartermijn van de persoonsgegevens

De persoonsgegevens worden zo lang als noodzakelijk bewaard voor de hierboven aangegeven doeleinden of zo lang als de wet dat voorschrijft. De Algemene Verordening Gegevensbescherming noemt geen concrete bewaartermijnen voor persoonsgegevens. In andere wetten kunnen wel minimale bewaartermijnen staan. Dan moeten die gegevens ook zo lang worden bewaard.

## Categorieën Medewerkers

|  |  |  |  |
| --- | --- | --- | --- |
| **Categorieën Medewerkers (functierollen/functiegroepen) van Verwerkers die Persoonsgegevens Verwerken** | **(categorie) Persoonsgegevens die door Medewerkers worden verwerkt** | **Soort Verwerking** | **Land van Verwerking** |
| Technisch- en applicatie beheer | 1, 2, 3, 6 | 1, 2, 3, 6 | NL |
| Service desk | 1, 2, 6 | 1, 2, 6 | NL |
| Financiën | 1, 2, 3, 4, 6 | 1, 2, 3, 4, 6 | NL |
| R&D | 5 | 5 | NL |

## Sub-verwerkers

Niet van toepassing

## Doorgiften

Niet van toepassing

## Contactgegevens

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Algemene contactgegevens**  | **Naam** | **Functie** | **E-mailadres** | **Telefoonnummer** |
| Verwerker | Pauline Terkoolt | Privacy Officer | privacy@xafax.nl | 072-5667400 |
|  |
|  | **Naam** | **Functie** | **E-mailadres** | **Telefoonnummer** |
| **Contactgegevens bij Inbreuk in verband met Persoonsgegevens** |  |  |  |  |
| Verwerker | Julian van Wickeren | Teamleider technisch- en applicatie beheer | jvwickeren@xafax.nl | 072-5667400 |

Bijlage 2: Beveiligingsmaatregelen

**Versie 2.1 – november 2018**

**Algemeen**

Verwerker heeft een passend beleid voor de beveiliging van de verwerking van de persoonsgegevens, waarbij de doeltreffendheid van de technische en organisatorische maatregelen periodiek wordt geëvalueerd en – zo nodig – aangepast.

Er is een informatiebeveiligingsbeleid opgesteld en er zijn met medewerkers afspraken gemaakt omtrent de naleving hiervan. Er zijn procedures opgesteld rondom risicobeoordeling en risicobehandeling, wijzigingsbeheer en incidentafhandeling.

De Verwerker hanteert een beleidsdocument dat expliciet ingaat op de maatregelen die de Verwerker treft om de verwerking van de gegevens te beveiligen, alsmede de privacy te waarborgen. Dit beleidsdocument is gebaseerd op algemeen gehanteerde beveiligingsstandaarden zoals de ISO 27002:2013.

**Geautoriseerde toegang tot persoonsgegevens**

In alle toepassingssystemen zijn beveiligingsmaatregelen ingebouwd waaronder een adequaat toegangsbeheer.

Verwerker hanteert een systeem van autorisatie waarbij enkel geautoriseerde medewerkers toegang kunnen verkrijgen tot de verwerking van persoonsgegevens. Hierbij heeft verwerker procedures vastgesteld voor de identificatie, autorisatie en authenticatie van medewerkers en rondom de registratie, aanmelding en afmelding van de medewerkers.

Verwerker heeft procedures voor het verlenen van toegang tot persoonsgegevens (waaronder een registratie- en afmeldprocedure voor toewijzing van toegangsrechten), en het in logbestanden vastleggen van gebeurtenissen betreffende gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen.

**Fysieke beveiliging**

De IT-voorzieningen en apparatuur zijn fysiek beschermd tegen toegang door onbevoegden en tegen schade en storingen.

**Geheimhouding**

De werknemers van de Verwerker die betrokken zijn bij de verwerking van persoonsgegevens zijn gehouden aan een geheimhoudingsplicht/integriteitscode.

**Training/scholing**

Alle werknemers van de organisatie en, voor zover van toepassing, ingehuurd personeel en externe gebruikers krijgen geschikte training en regelmatige bijscholing over het informatiebeveiligingsbeleid en de informatiebeveiligingsprocedures van de organisatie, voor zover relevant voor hun functie. Binnen de training en bijscholing wordt expliciet aandacht besteed aan de omgang met (bijzondere categorieën van; of anderszins gevoelige) persoonsgegevens.

**Wachtwoordbeleid**

Er is een authenticatie- en wachtwoordbeleid met verplicht gebruik van sterke wachtwoorden en/of 2FA om bevoegde gebruikers toegang te geven tot de informatiesystemen en -diensten die ze voor de uitvoering van hun taken nodig hebben en om onbevoegde toegang tot informatiesystemen te voorkomen.

**Beveiligingsincidenten**

Er is een procedure voor het tijdig en doeltreffend behandelen van informatiebeveiligingsincidenten en zwakke plekken in de beveiliging, zodra ze zijn gerapporteerd.

**Back-up**

Er is voorzien in een adequate back-up en recovery procedure om corruptie of ongewenst verlies van (persoons-)gegevens te kunnen herstellen.

Er is een bedrijfscontinuïteitsplan opgesteld om de continuïteit van de dienstverlening bij uitval van systemen te waarborgen .

**Monitoring**

Het netwerk en de informatiesystemen worden actief gemonitord en beheerd om onbevoegde informatieverwerkingsactiviteiten te ontdekken. Er is een procedure ingesteld over de omgang met en de afhandeling van datalekken. Onderdeel hiervan is het informeren van de Verwerkingsverantwoordelijke.

De Verwerker installeert tijdig oplossingen die de leveranciers uitbrengen voor beveiligingslekken. Dit alles uitsluitend indien en voor zover de betreffende software door de Verwerker is/wordt geleverd, of gebruikt, of onderhouden ten behoeve van de Verwerkingsverantwoordelijke.

Er is een procedure ingesteld om applicaties up-to-date te houden.

**Testen op kwetsbaarheden**

Verwerker heeft maatregelen genomen om zwakke plekken te identificeren ten aanzien van de verwerking van persoonsgegevens in de systemen. Zo wordt er regelmatig getest op technische kwetsbaarheden binnen het netwerk en omliggende systemen.

Waar mogelijk is antivirus en antimalware software geïnstalleerd en actief.

**Persoonsgegevens**

Verwerker heeft de persoonsgegevens die worden verwerkt geclassificeerd op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid en heeft op basis van die classificatie beveiligingsmaatregelen genomen om de risico’s voor de verwerking van persoonsgegevens te beperken.

Bij transport en opslag van door de Verwerkingsverantwoordelijke expliciet als zodanig aangemerkte vertrouwelijke informatie over netwerken wordt altijd adequate encryptie toegepast.

Bijlage 3: Procedure Datalekken

**Versie 1.1 – 24-5-2019**

Een beveiligingsincident (hierna datalek) is een inbreuk, opzettelijk of per ongeluk, in verband met persoonsgegevens. Er is sprake van een datalek als er een inbreuk is op de beveiliging die als gevolg heeft:

* vernietiging (definitief) van persoonsgegevens (bijvoorbeeld door brand of wissen); of
* verlies van persoonsgegevens (bijvoorbeeld USB of laptop die kwijtraakt); of
* wijziging van persoonsgegevens (zonder dat dit de bedoeling was); of
* ongeoorloofde verstrekking van persoonsgegevens (bijvoorbeeld e-mail/bestanden verzonden aan verkeerde geadresseerde); of
* ongeoorloofde toegang tot doorgezonden/opgeslagen/anderszins verwerkte persoonsgegevens (bijvoorbeeld door een hacker of een niet-bevoegd personeelslid).

Tussen Partijen zijn met betrekking tot de meldplicht datalekken de volgende afspraken gemaakt:

Stap 1: Xafax stelt vast of er sprake is van een datalek;

Stap 2: Het privacyteam van Xafax bespreekt het datalek en de te nemen acties. Het privacyteam van Xafax bestaat uit: directielid, teamleider technisch- en applicatie beheer en de Privacy Officer;

Stap 3: Xafax neemt maatregelen volgens de vragenlijst om het (actieve) lek te stoppen of de gevolgen te beperken;

Stap 4: Xafax onderzoekt en verzamelt zo veel mogelijk gegevens omtrent het datalek;

Stap 5: Xafax informeert verwerkingsverantwoordelijke zonder onredelijke vertraging en zal de relevante informatie over het incident melden aan de hand van de hierna opgenomen vragenlijst;

Stap 6: Xafax neemt maatregelen om eenzelfde soort datalek in de toekomst te voorkomen;

Stap 7: Verwerkingsverantwoordelijke zal beoordelen of een melding verricht dient te worden bij de AP. Verwerkingsverantwoordelijke zal daarbij in overleg treden met Xafax;

Stap 8: Voordat verwerkingsverantwoordelijke de melding bij de AP verricht zal verwerkingsverantwoordelijke de inhoud van de melding met Xafax bespreken;

Stap 9: Indien verwerkingsverantwoordelijke oordeelt dat tevens betrokkenen geïnformeerd dienen te worden over het datalek, zal verwerkingsverantwoordelijke de inhoud van die informatie met Xafax bespreken.

**Vragenlijst datalek – bij procedure meldplicht datalekken**

1. **Contactgegevens**

Verwerkersverantwoordelijke:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | Functie | Telefoon | E-mail |
| Naam 1e contactpersoon |  |  |  |  |
| Naam 2e contactpersoon |  |  |  |  |

Xafax (verwerker):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | Functie | Telefoon | E-mail |
| Naam 1e contactpersoon | Julian van Wickeren | Teamleider technisch- en applicatie beheer | 072-5667400 | privacy@xafax.nl |
| Naam 2e contactpersoon | Pauline Terkoolt | Privacy Officer | 072-5667400 | privacy@xafax.nl |

1. **Wat is het voor datalek:**

….(invullen door Xafax)

Kies er 1:

* Apparaat, gegevensdrager (bijv. USB-stick) en/of papier met persoonsgegevens kwijtgeraakt of gestolen;
* Brief of postpakket met persoonsgegevens kwijtgeraakt of geopend retour ontvangen;
* Ongeoorloofde toegang tot doorgezonden/opgeslagen/anderszins verwerkte persoonsgegevens (bv hacker, malware, phishing of niet bevoegd personeel).
* Persoonsgegevens per ongeluk gewijzigd of definitief verwijderd;
* Vernietiging van persoonsgegevens (bv brand of wissen);
* Persoonsgegevens nog aanwezig op afgedankt apparaat of op afgedankte gegevensdrager (bijv. USB-stick);
* Persoonsgegevens per ongeluk gepubliceerd;
* Persoonsgegevens van verkeerde klant getoond in klantportaal;
* Persoonsgegevens verstuurd of afgegeven aan verkeerde ontvanger;
1. **Geef een samenvatting van het datalek:**

….(invullen door Xafax)

1. **Indien het datalek plaatsvond bij een sub-verwerker:**

….(naam sub-verwerker)

1. **Van hoeveel personen zijn persoonsgegevens betrokken bij het datalek?**

Minimaal….(invullen door Xafax)

Maximaal….(invullen door Xafax)

1. **Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij het datalek:**

….(invullen door Xafax)(bv leerlingen, ouders, medewerkers, gasten)

1. **Wanneer vond het datalek plaats?**

Op (datum)….(invullen door Xafax)

Tussen (begindatum) en (einddatum)

Nog niet bekend

1. **Wanneer is het datalek ontdekt?**

….(invullen door Xafax)

1. **Wat is de aard van het datalek? Omcirkel de antwoorden en vul in waar nodig**
* Kan een onbevoegde de gegevens lezen: ja/nee
* Kunnen/zijn de gegevens (worden) gekopieerd door een onbevoegde: ja/nee
* Kunnen/zijn de (bron)gegevens (worden) gewijzigd (bv hack in het systeem): ja/nee
* Kunnen/zijn de (bron)gegevens (worden) verwijderd of vernietigd

(bv. ransom ware of brand datacenter): ja/nee

* Zijn de gegevens gestolen: ja/nee
1. **Om welk type gegevens gaat het? Omcirkel de antwoorden en vul in waar nodig:**
* Identificatiegegevens, zoals naam, achternaam, geslacht en geboortedatum: ja/nee
* Contactinformatie, zoals (e-mail)adres en (mobiel) telefoonnummer: ja/nee
* Transactiegegevens, zoals bijschrijvingen en afschrijvingen: ja/nee
* Financiële gegevens, zoals bankrekeningnummer (in geval betrokkene

restitutie wil aanvragen): ja/nee

* Gegevens over online gedrag en voorkeuren, zoals het IP-adres mobiele

apparaat of computer en de pagina’s die betrokkene op de website of in de

apps van Xafax bezoekt: ja/nee

* Gegevens die betrokkene deelt met onze contactdiensten, correspondentie

met Xafax en support data (telefoon, chatgesprekken en e-mail): ja/nee

1. **Welke gevolgen kan het datalek hebben voor de getroffen personen? Omcirkel de antwoorden en vul in waar nodig:**
* Stigmatisering of uitsluiting: ja/nee
* Schade aan de gezondheid: ja/nee
* Kans op identiteitsfraude: ja/nee
* Kans op financiële schade (bv fraude met creditcardgegevens): ja/nee
* Blootstelling aan spam of phishing: ja/nee
* Andere gevolgen, namelijk:
1. **Omschrijf welke technische en organisatorische maatregelen zijn getroffen om het datalek aan te pakken, om de eventuele nadelige gevolgen ervan te beperken en om verdere inbreuken te voorkomen en, zoveel mogelijk en indien van toepassing, de maatrelen die worden voorgesteld om in de toekomst nog toe te passen met deze doeleinden?**

….(invullen door Xafax)

1. **Zijn de gelekte persoonsgegevens beveiligd? Omcirkel de antwoorden en vul in waar nodig:**

Zijn de gegevens versleuteld:

Zo ja; welke versleuteling: ….(invullen door Xafax)

Geldt deze versleuteling voor alle persoonsgegevens of voor een deel? Indien voor een deel, voor welk deel: ….(invullen door Xafax)

Zijn de gegevens gehasht:

Zo ja; op welke wijze: ….(invullen door Xafax)

Kunnen de gegevens vanaf afstand worden gewist:

Zo ja; is dat gebeurd en wanneer is dat gebeurd: ….(invullen door Xafax)

Zijn de gegevens op een andere manier onbegrijpelijk of ontoegankelijk gemaakt:

Zo ja; op welke manier: ….(invullen door Xafax)

1. **Zijn er persoonsgegevens van personen in andere EU-landen getroffen door het datalek? Zo ja, welke uit welke landen:**

….(invullen door Xafax)