phenoxconsultants
actuaries › employee benefits

Beveiligingsmaatregelen Data Phenox Consultants B.V.

1. Organisatorische maatregelen

1.1. Phenox werkt zonder fysiek archief; privacy gevoelige persoonsgegevens (hierna: gegevens) worden alleen elektronisch opgeslagen.

1.2. De Privacy Officer (hierna: PO) is de kantoorverantwoordelijke persoon. In noodsituaties kan een nader door deze kantoorverantwoordelijke aan te wijzen andere persoon kortstondig rechten worden toegekend. In uitzonderlijke noodsituaties zou ook de IT-beheerder aangewezen kunnen worden

1.3. Indien privacygevoelige informatie aan de klant wordt geleverd zal dit in principe plaatsvinden m.b.v. de speciaal hiervoor ingerichte klantportal volgens de bijbehorende interne richtlijnen voor een “file transfer”, waaronder:

1.3.1. Te versturen bestanden zijn altijd versleuteld en beveiligd met een wachtwoord.

1.3.2. De medewerker dient de klant expliciet kenbaar te maken dat wachtwoorden bij voorkeur via WhatsApp (in verband met end-to-end encryptie) worden verstuurd, en alleen naar vooraf afgestemde en goedgekeurde telefoonnummers.

Alleen op uitdrukkelijk verzoek van de klant kunnen - bij hoge uitzondering - bestanden als bijlage van een email verstuurd worden.
Indien de klant er zelf nadrukkelijk voor kiest het wachtwoord per e-mail, sms of anderszins te laten versturen zijn de daaruit voortvloeiende aanvullende veiligheidsrisico’s voor rekening van de klant.

1.4. Indien medewerkers de klanten vragen om privacy gevoelige informatie en/of noodzakelijke persoonsgegevens dienen zij de klant te verzoeken dit op vergelijkbaar veilige wijze te doen.

Alle aanvullende veiligheidsrisico’s die in het kader van AVG voortvloeien uit onveilig en niet conform de richtlijnen handelen door de klant komen voor rekening van de klant. Phenox Consultants BV kan op generlei wijze aansprakelijk worden gesteld voor het handelen van de klant, en derhalve ook niet voor de gevolgen van het toesturen, (tijdelijk) bezit én mogelijke weer doorsturen door Phenox Consultants BV van deze niet-noodzakelijke persoonsgegevens.
Dit kan bijvoorbeeld - niet uitputtend - zijn als de klant er voor kiest:

1.4.1. ongevraagd niet-noodzakelijke persoonsgegevens te versturen;

1.4.2. persoonsgegevens gegevens en/of wachtwoorden per e-mail, sms of anderszins verstuurt of laat versturen;

1.4.3. derden, zoals externe pensioenuitvoerders, vraagt gegevens te leveren;

1.4.4. persoonsgegevens in algemene zin onveilig verstuurt of laat versturen.

1.5. Het al dan niet naleven van voorgaande en hierna volgende werkafspraken voor Phenox medewerkers laat onverlet dat artikelen 1.3 en/of 1.4 van kracht zijn op deze gegevens.

1.6. Ontvangen gegevens worden door de betrokken werknemers bij ontvangst gescreend op het doel waarvoor zij gebruikt dienen te worden. Ontvangen gegevens die niet noodzakelijk zijn voor de uit te voeren taken worden zoveel mogelijk direct verwijderd.

In dit geval stelt de betrokken medewerker de klant en PO op de hoogte van het verwijderen van deze gegevens.

1.7. Gegevens die per post worden ontvangen, worden indien noodzakelijk als pdf gescand en in de betreffende elektronische klantenmap bewaard. In alle gevallen worden fysieke gegevens zo snel mogelijk weggegooid middels een speciaal daartoe aanwezige afgesloten container, waarvan de inhoud door een gespecialiseerd bedrijf vernietigd wordt.

1.8. Phenox medewerkers werken op basis van “clean desk” policy, wat wil zeggen dat (mogelijk privacygevoelige) informatie niet fysiek bewaard mag worden en alleen in uitzonderingsgevallen voor korte periodes in fysieke vorm aanwezig kan zijn, bijvoorbeeld in geval van notities gedurende een opdracht. In dat geval wordt deze (tijdelijke) informatie achter slot bewaard bij het verlaten van de werkplek of alsnog verwerkt conform lid 1.5.

1.9. Ontvangen gegevens worden opgeslagen in de desbetreffende (digitale) klantenmap. Alleen medewerkers die direct verbonden zijn aan de klant hebben toegang tot de elektronische map, waarin gegevens van de desbetreffende klant worden opgeslagen. Deze lijst met bevoegdheden wordt bewaard en up-to-date gehouden door de PO.

1.10. Gegevens die niet langer relevant zijn voor de uit te voeren opdracht, zoals ontvangen bronbestanden, worden in de per klant aanwezige extra beveiligde archiefmap bewaard. Deze mappen zijn als uitgangspunt voor niemand toegankelijk. Indien toegang om welke reden ook noodzakelijk blijkt, kan dit alleen via de PO.

1.11. Medewerkers dienen de PO te informeren in geval van twijfel over de staat van de bescherming van de gegevens of in geval van mogelijk of daadwerkelijk lekken van de gegevens, bewust of onbewust.

1.12. Waar het de gegevens van de medewerkers betreft hebben alleen de kantoorverantwoordelijke en secretaresse toegang tot de relevante elektronische mappen.

1.13. Van medewerkers worden geen fysieke gegevens bewaard. Indien er vanwege zwaarwegende of wettelijke gronden wel fysieke informatie wordt bewaard, dan verplicht de werkgever zich:
1.13.1. de betrokken werknemer hiervan op de hoogte te stellen;
1.13.2. de fysieke gegevens achter slot en grendel te bewaren.

2. Technische maatregelen

2.1. Alle devices (computers, laptops, telefoons, tablets, etc.) zijn voorzien van up-to-date antivirussoftware en actief beheer. Zie het document: Beheerplan IT systemen Phenox Consultants BV

2.2. Actief patch/updatebeleid alle systemen.

2.3. Alle devices (computers, laptops) die mogelijk privacygevoelige data kunnen bevatten zijn voorzien van encryptie en beveiligd met sterke wachtwoorden (minimaal 8 karakters) of vergelijkbaar sterk alternatief.

2.4. Alle mobiele devices (telefoons, tablets, e.d.) zijn voorzien van encryptie en beveiligd met sterke wachtwoorden (minimaal 6 karakters) of vergelijkbaar sterk alternatief zoals bijvoorbeeld vingerafdrukscan of Face ID.

2.5. Mobiele devices zoals laptops, tablets of telefoons dienen niet onbewaakt (o.a. in de auto) achtergelaten te worden

2.6. Bij afwezigheid dienen alle devices vergrendeld te zijn.

2.7. Alle devices zijn voorzien van een automatische vergrendeling bij afwezigheid.

2.8. Gebruik van mobiele datadragers (o.a. USB Sticks, Cd's) is in de regel niet toegestaan. Indien noodzakelijk voor de uitvoering van de taken kan hiervoor een uitzondering worden gemaakt, dit gebeurt enkel met toestemming van de PO. In dat geval zal Phenox de medewerker voorzien van een versleutelde en beveiligde oplossing.

2.9. Gebruik van privé devices en elke vorm van gegevensopslag (inclusief, maar niet beperkt tot, e-mail) op privé devices (o.a. computers, mobiele devices) is nadrukkelijk niet toegestaan.

2.10. Gebruik van- of toesturen van gegevens naar privé e-mailadressen of andere privé gegevensopslag is nadrukkelijk niet toegestaan

2.11. Onbeveiligde apparaten zijn nadrukkelijk niet toegestaan binnen Phenox

2.12. Communicatie via e-mail is alleen beveiligd toegestaan

3. Website maatregelen

3.1. Communicatie via de website, bijvoorbeeld via een contactformulier, dient met encryptie beveiligd te zijn.

3.2. Phenox voert een actief updatebeleid voor eigen en gerelateerde websites.

3.3. Medewerkers betrokken bij het aanpassen van de websites dienen zich te verzekeren dat er geen gevoelige informatie via de website bekend wordt gemaakt.

4. Backup maatregelen

4.1. Alle data dient lokaal (op de Phenox servers) te worden versleuteld en alleen versleuteld naar de externe back-up server verzonden.

4.2. De Data is 2048-bit AES-128 versleuteld.

4.3. De, voor herstel van de back-up, benodigde decryptiesleutel is enkel in het bezit van de PO. Deze wordt bewaard in de daarvoor bestemde extra beveiligde digitale locker, met een reservekopie in de bij Phenox aanwezige kluis.
Deze is derhalve niet direct toegankelijk door de hosting partij noch door derden.

4.4. Om ongeoorloofd gebruik van eventueel ontvreemde decryptiesleutel tegen te gaan is de back-up server voorzien van een extra authenticatie laag.

4.5. De back-up wordt real-time bijgewerkt en is voorzien van “versioning”, ofwel worden meerdere, eerdere versies van hetzelfde bestand bijhouden om onbedoelde opgeslagen wijzigingen te kunnen herstellen.

5. Server maatregelen

5.1. De server wordt beschermd door een actieve firewall.

5.2. De server is voorzien van up-to-date antivirussoftware

5.3. Er is sprake van een actief patch- en updatebeleid op de server

5.4. De server is voorzien van een (beperkte) log feature met betrekking tot toegang door externe gebruikers

5.5. De server wordt actief beheerd op toegangsrechten conform artikel 1.5

5.6. De server voorziet in een back-up mogelijkheid zoals uiteengezet in artikel 5.