

Bijlage 1

Persoonsgegevens die verwerkt worden door Verwerker (niet limitatief)

- E-mailadres
- Voornaam
- Achternaam
- Doopnamen
- Adres
- Postcode
- Woonplaats
- Telefoonnummer (zowel mobiel als vast)
- Geslacht
- Burgerlijke staat
- Geboorteplaats
- CV's/CV gegevens
- Kopie paspoort/paspoort gegevens
- Kopie rijbewijs/ rijbewijs gegevens
- Kopie loonstrook/loonstrook gegevens
- Sofinummer/BSN
- Bankrekeningnummer/IBAN
- Creditcardnummer
- Handelsregisternummer
- Overeenkomsten
- Verzekeringopolis
- Klantnummer
- Factuurnummer
- Relatienummer
- Loginnaam
- Wachtwoorden
- Gezondheid (voor zover nodig voor ziektekostenaftrek inkomstenbelasting)
- Lidmaatschapsgegevens
- Social media accounts
- Profielfoto
- Videobeelden
- Kentekens
- Telecomgegevens
- Verkeersgegevens
- Gegevens bedrijf/ bedrijfsnaam
- Gegevens simkaart
- Unieke apparaat nummers
- Serienummers software
- WWFT check/recherche check
- Cliënt groep (bijdrage aan de omzet)
- Financiële informatie (aangiftes/aanslagen)
- Niet geanonimiseerd bezwaar/beroep

Betrokkenen (niet limitatief)

- Werknemers
- Familierelaties/partners van werknemers
- Cliënten
- Familierelaties/partners van cliënten
- Zakelijke contacten, waaronder o.a. Belastingdienst-/UWV-/gerechtmedewerkers, medewerkers concullega's, externe advocaten en juristen, bankmedewerkers

Bijlage 2Technische en organisatorische beveiligingsmaatregelen

De genoemde maatregelen dienen om de betrouwbaarheid, integriteit en beschikbaarheid van de systemen en diensten met betrekking tot de verwerking, op permanente basis te garanderen en ervoor te zorgen dat de beschikbaarheid van en toegang tot persoonsgegevens in het geval van een fysiek of technisch incident snel kan worden hersteld.

1. Technische bescherming van de Wesselman werkomgeving

De toegang tot de werkomgeving van de verwerker wordt beschermd door authenticatie op basis van twee factoren. Sterke wachtwoorden worden afgedwongen, bij voorkeur door technische controles (uniek wachtwoord, hoofdletters/kleine letters, cijfers, niet-alfanumerieke tekens en minimaal 7 tekens). Binnen onze cloud omgeving hebben we onze bedrijfsapplicaties beschikbaar (zoals AFAS, Exact Online, Loket.nl) via een federatief account management systeem.

De accounts van onze medewerkers worden beheerd via een IAM-toepassing (Identity and Access Management) die ons HR-systeem gebruikt als referentiepunt voor medewerkers en hun autorisaties. Alle autorisaties zijn gebaseerd op functie, afdeling, rollen en juridische entiteit waar de medewerker deel van uitmaakt. Wijzigingen worden automatisch toegepast wanneer er een wijziging wordt aangebracht in het HR-systeem.

Met behulp van aanvullende beveiligingsmaatregelen beperken we de toegang tot gegevens buiten onze cloud omgeving. Mailboxen zijn alleen toegankelijk via onze cloud werkomgeving, mobiele apparaten of versleutelde laptops. De medewerker is verplicht om een wachtwoord/toegangscade of 2-factor authenticatie te gebruiken. Indien nodig kunnen we bovengenoemde apparaten op afstand wissen.

2. Interne organisatorische veiligheidsmaatregelen

Verwerker past een strikt lock-screen beleid toe om gevoelige gegevens te beschermen en automatische screensavers met wachtwoordbeveiliging zijn actief. Er wordt actief aandacht besteed aan de bewustwording van het gebruik van gevoelige gegevens door zijn werknemers en er is een strikt wachtwoordbeleid van kracht.

Om gegevens af te drukken is een speciale autorisatie (printerpin) nodig of het gebruik van de tag aan de van de werknemer.

Persoonlijke gegevens worden alleen gebruikt voor het aangegeven doel.

Papier wordt afgevoerd via de sleuf van verzegelde containers die daarvoor bestemd zijn. Deze containers worden regelmatig geleegd door een derde partij, volgens de strengste wettelijke DIN / ISO 66399-norm evenals ISO 9001-2015, ISO/IEC 27001, ISO 50001, ISO/IEC 21964-2018, OPK en CA+.

De verwerker heeft protocollen en procedures om ervoor te zorgen dat informatiebeveiligingsincidenten tijdig en effectief worden afgehandeld. Het ziet ook toe op de naleving van protocollen en wet- en regelgeving.

3. Netwerk- en internetbeveiliging en logboekregistratie

Processor maakt gebruik van een beschermde digitale omgeving, waarin alle netwerkactiviteiten worden gelogd en gemonitord. Deze omgeving wordt beschermd door firewalls, threat intelligence monitoring, IPS en virusscanners om optimale beveiliging te bereiken. Er zijn gedefinieerde verantwoordelijkheden op het gebied van gegevensbescherming en IT-beveiliging en om mogelijke risico's voor gegevens en systemen te detecteren en aan te pakken. Alle toegang en wijzigingen worden geregistreerd en opgeslagen op een centrale beveiligingsserver. Onze externe partners hebben op verzoek logboeken beschikbaar op gebruikers- en tijdstempelniveau.

De kring van functionarissen die toegang hebben tot bepaalde persoonsgegevens is beperkt tot alleen die personen die toegang tot de persoonsgegevens nodig hebben voor de uitoefening van hun functie. Ook hebben werknemers ingestemd met een geheimhoudingsclausule met bijbehorende boeteclausule.

Toegangsrechten van werknemers worden ingetrokken bij ontslag of verandering van afdeling. De gegevenstoegangsrechten worden regelmatig herzien. Medewerkers worden grondig geïnstrueerd en getraind in het gebruik van de gegevens van de Verwerker.

- Gegevens (en kopieën daarvan) worden alleen versleuteld opgeslagen op niet-vluchtige opslag.
- Gegevens (en kopieën daarvan) worden alleen versleuteld overgedragen in netwerken.

4. Herstelbaarheid

Ervoor zorgen dat systemen die in gebruik zijn, hersteld kunnen worden in het geval van een storing, De verwerker neemt de volgende maatregelen:

- De processor maakt regelmatig back-ups van de gegevens, waaruit de gegevens kunnen worden verwijderd of systemen kunnen worden hersteld.
- Er worden rampenplannen opgesteld om op dergelijke incidenten te reageren.
- De servers:
 - worden virtueel bediend en worden 24/7 bewaakt met monitoringtools.
 - Data wordt dagelijks geback-upt, er wordt een bewaarperiode van 30 dagen gehanteerd, de back-ups worden opgeslagen in aparte afgesloten ruimten en veilig bewaard tegen diefstal, vernietiging of gegevensverlies.

5. Software partners

Verwerker maakt gebruik van AFAS-software en heeft Ictivity als IT-partner. Beide partijen beschikken over certificeringen die adequate up-to-date beveiligingsmaatregelen op het gebied van informatiebeveiliging garanderen. Ictivity en AFAS werken beide volgens ISO/IEC 27001, de bekendste norm voor informatiebeveiligingseisen.

AFAS past de ISAE 3402 standaard toe voor kwaliteits- en veiligheidscontrole van AFAS online en de MJA-3 standaard voor het testen van de kwetsbaarheid van systemen voor aanvallen.

Onze salarisadministratie gebruikt het softwarepakket Loket.nl, dat ook de ISAE 3402-standaard toepast. Servers die relevant zijn voor Loket.nl bevinden zich in datacenters die voldoen aan minimaal ISO/IEC 27001.

Onze boekhoudafdeling gebruikt boekhoudsoftware van verschillende softwarepartners, zoals Exact Nederland B.V., maar ook Caseware B.V. en Unit4 Bedrijfssoftware B.V. Alle bovengenoemde software is alleen beschikbaar via ons federatieve accountsysteem en autorisaties.

Dit betekent dat er passende informatiebeveiligingsmaatregelen worden genomen in overeenstemming met de GDPR.

6. Fysieke beveiliging

De faciliteiten en kantoren van Processor zijn voldoende beveiligd. De locaties van Processor hebben een alarmsysteem, ondersteund door een responsprotocol en een toegangscontrolesysteem.

Tijdens openingstijden, maandag t/m vrijdag van 08:15 tot 17:00 uur, zijn de voordeuren van de locaties niet op slot, de receptie met direct zicht op deze deur is in deze periode bezet. Bezoekers moeten opgehaald worden bij de receptie en begeleid worden tijdens hun bezoek. Aan de buitenkant van het pand in Helmond hangen camera's die 14 dagen worden bewaard. Ze zijn alleen zichtbaar voor IT-medewerkers en bestuursleden.

Op alle locaties is een digitaal sluitsysteem geïnstalleerd en toegepast op binnendeuren. Elke medewerker heeft een unieke badge die is toegewezen aan de medewerker en gekoppeld aan bepaalde toegangsrechten en tijden.

Alle openingen, weigeringen en updates worden geverifieerd en opgeslagen op een netwerkserver buiten het gebouw. Badges worden ingetrokken zodra ze zoekraken, meer dan 30 dagen niet zijn gebruikt of een medewerker wordt ontslagen.

Bestuursleden en eigenaren hebben 24 uur per dag volledige toegang tot het pand. Medewerkers hebben alleen toegang tijdens kantooruren en alleen IT-medewerkers hebben toegang tot de serverruimtes. IT-medewerkers maken en geven badges aan medewerkers.