

Bijlage J - Informatiebeveiliging Privacy (AVG)

Een werkgever heeft de verplichting om van alle werknemers een personeelsdossier bij te houden.

Het personeel moet erop kunnen vertrouwen dat er zorgvuldig met die gegevens omgegaan wordt en dat deze gegevens niet voor iedereen toegankelijk zijn.

Naast de standaardgegevens (NAW, contactgegevens, functiegegevens, enz.) bevat een personeelsdossier veel gevoelige/bijzondere persoonsgegevens, zoals financiële gegevens, gezondheidsgegevens, Burgerservicenummer, enz..

Het verwerken van deze gevoelige/bijzondere gegevens brengt een verhoogd risico van misbruik met zich mee die potentieel grote impact op de betrokkene heeft en daarmee vraagt om een hoog beveiligingsniveau.

Verwerker, subverwerker en verwerkersovereenkomst

De leverancier (verwerker) moet kunnen aantonen dat de juiste technische en organisatorische maatregelen zijn genomen om de persoonsgegevens te beveiligen.

Met de leverancier dient een verwerkersovereenkomst afgesloten te worden. Hiervoor wordt gebruik gemaakt van de meest actuele VNG Standaard verwerkersovereenkomst.

Het is mogelijk dat de verwerker bepaalde diensten uitbestede heeft, zoals bijvoorbeeld de opslag van de gegevens bij een datacenter. De verwerker dient duidelijke informatie te verstrekken over deze subverwerker.

- NAW gegevens
- Overzicht van de uitbestede taken (beheer, back-up, helpdesk, enz.)
- Certificering subverwerker

Dataminimalisatie

Het beginsel van minimale gegevensverwerking (dataminimalisatie) is een van de belangrijkste beginselen onder de AVG. Wanneer persoonsgegevens worden verwerkt dan moeten zij voor het doel toereikend en ter zake dienend zijn. Verder mogen er niet meer persoonsgegevens worden verwerkt dan noodzakelijk voor het doel.

Sommige persoonsgegevens mogen beslist niet vastgelegd worden. Informatie over iemands ras, politieke voorkeur, seksuele geaardheid, godsdienst en vakbondslidmaatschap hoort bijvoorbeeld niet thuis in het personeelsdossier. Ook is het verboden om medische gegevens op te nemen.

Bewaartermijn

Om een goede administratie bij te kunnen houden, moet een organisatie bepaalde persoonsgegevens een tijd bewaren. In principe mogen organisaties die gegevens niet langer bewaren dan noodzakelijk. Wel moet de organisatie zich houden aan de concrete bewaartermijnen vermeld in andere wetten, zoals bijvoorbeeld de belastingwetgeving, archiefwetgeving etc. (zie selectielijst gemeenten).

Functiescheiding en autorisatie

Het personeelsdossier bevat gevoelige persoonsgegevens en verder vertrouwelijke informatie. Werknemers verwachten van dat daar op gepaste wijze mee omgegaan wordt. Zorg er daarom voor dat de dossiers niet voor iedereen toegankelijk zijn.

Geef alleen toegang aan medewerkers die deze informatie nodig hebben om hun werk goed te kunnen doen, zoals leidinggevend en medewerkers van Personeelszaken.

Ter verantwoording (BIG/BIO) dient het systeem op eenvoudige wijze een autorisatiematrix aan te kunnen aanleveren t.b.v. de CISO.

Rechten van betrokkenen

Mensen hebben verschillende rechten om controle te houden over hun persoonsgegevens. Gehoor geven aan mensen die een beroep doen op hun privacyrechten is een belangrijk onderdeel van een gezond privacybeleid. En een gezond privacybeleid draagt bij aan het vertrouwen van mensen in uw organisatie.

- Recht op inzage.
- Recht op vergetelheid
- Recht op rectificatie en aanvulling
- Het recht op dataportabiliteit
- Het recht op beperking van de verwerking
- Het recht met betrekking tot geautomatiseerde besluitvorming en profilering
- Het recht om bezwaar te maken tegen de gegevensverwerking.
- Ten slotte hebben mensen recht op duidelijke informatie over wat u met hun persoonsgegevens doet

Systemen (en ook processen en interne organisatie) dienen ingericht te zijn op deze rechten, zodat op een juiste en eenvoudige manier gehoor gegeven kan worden aan verzoeken van betrokkenen.

Informatiebeveiliging

U gaat akkoord met een Intrusion & Detection test, in overleg uit te voeren door een gecertificeerde medewerker van de aanbestedende dienst of door inschrijver aan te wijzen extern adviesbureau. Tevens dient het systeem te voorzien in dataclassificatie.