

PIA informatie

PIA

e-HRM-

Auteursnaam

Naam van de beoordelaar

Validator's naam

Aanmaakdatum

29/03/2021

Naam FG

FG

Mening FG

Geaccepteerde DPIA

Zoeken naar de mening van betrokkenen

Mening van betrokkenen werd gevraagd.

Namen van betrokkenen

Statussen van betrokkenen

De gegevensverwerking zou kunnen worden geïmplementeerd.

Concerned people opinions

Deelnemers aan de DPIA-sessie zijn van mening dat er voldoende maatregelen zijn genomen om de verwerking met de betreffende systemen uit te voeren. Aanscherping van enkele maatregelen kan het risico verlagen.

Bijlagen

<div><div>systemschets e-Hrm omgeving.pptx</div><div>verkeerde extensie</div></div>
<div><div>systemschets e-Hrm omgeving.pptx</div><div>verkeerde extensie</div></div>
<div><div>systemschets e-Hrm omgeving.pdf</div></div>
<div><div>Bijlage 1c Verwerkersovereenkomst Provincie Limburg en <div></div> Software.pdf</div></div>

Overzicht

Welke gegevensverwerking wordt overwogen?

Het betreft de gegevensverwerking ter ondersteuning van het HRM-proces.
Hieronder vallen:

- personeelsregistratie;
- organisatie, formatie en bezetting;
- beoordelen en belonen (het goede gesprek);
- salarisadministratie;
- declaratieverwerking;
- verlofadministratie;
- verzuimadministratie;
- individueel keuze budget (IKB) administratie;
- werving en selectie;
- ()
- digitaal personeelsdossier;
- archivering;
- uitvoering Wet Banenafpraak (participatiewet);
- pensioenregeling;
- opting in/out/arbeidsvoorwaarden politieke ambtsdragers;
- arbeidsduur en werktijden;
- ontslag en uitkering;
- innen vorderingen/betalingen aan derden;
- VOG;
- registreren en verwerken van sollicitaties n.a.v. opengestelde vacatures;
- registratie externe en ingehuurd medewerkers (excl kosten).

Wat zijn de doeleinden van de gegevensverwerkingen?

Het hoofddoel van de verwerking is het ondersteunen van HRM-proces, zodat voldaan wordt aan de wettelijke verplichtingen als werkgever. De verwerking is daarmee een randvoorwaarde voor de interne bedrijfsvoering. Dit bevat onder andere:

- In- door- en uitstroom van (nieuwe)medewerkers, stagiaires en bestuurders;
- Registeren externe of ingehuurd medewerkers;
- Inhuur/in dienst nemen medewerkers in het kader Wet banenafpraak (participatiewet);
- Uitvoeren van de Arbeidsvoorwaarden CAP;
- Uitvoeren Pensioenregeling;
- Uitvoeren arbeidsvoorwaarden politieke ambtsdragers;
- Gerelateerde zaken rondom verzuim;
- Registratie, toetsing en begeleiding re-integratie;
- Toetsing strafrechtelijk verleden (VOG);
- Identificatieverplichting (identiteitsbewijs);
- Werven en selecteren van nieuwe medewerkers;
- Loonheffing;
- Uitvoeren wettelijke plichten.

Waar vinden de gegevensverwerkingen plaats?

E-Hrm bestaat uit een viertal systemen die gehost worden bij . Het betreft , , en . Daarnaast wordt gebruik gemaakt van een en b .

Vanuit wordt gebruik gemaakt van subverwerkers (). Verwerking vindt plaats binnen de EER.

Welke verantwoordelijkheden zijn verbonden aan de gegevensverwerking?

Het systeem wordt gebruikt door:

- personeelslid (muteren basisgegevens);
- management (muteren verzuim, verlof, declaraties, nieuwe medewerkers, gratificatie, functiewijzigingen, arbeidsvoorwaarden wijzigingen, overplaatsingen, uitdienst);
- Hr-adviseurs cluster P&O (ondersteuning management);
- medewerker personeelsbeheer (muteren formatie, bezetting, opstellen arbeidsvoorwaarden incl. wijzigingen)
- medewerker salarisadministratie (muteren salarisgegevens);
- medewerkers rechtspositie (raadplegen, adviseren, controleren);
- functioneel beheer (functionele aanpassingen, rapportages ed.);
- technische beheer (beschikbaarheid van het systeem);
- helpdesk (mutatie emailadressen, accountnamen)
- arbodienst (muteren verzuimgegevens);
- secretariaat (verzuimmeldingen);
- financiën(declaraties, journaalposten)
- control (ao, derde lijncontrole)

Binnen het systeem worden de verantwoordelijkheden vertaald in de autorisaties voor functionaliteiten (rollen).

Welke wet- en regelgevingen hebben betrekking op de gegevensverwerkingen?

De gegevensverwerking is niet in strijd met de

- ambtenarenwet;
- WNRA;
- CAO-provincies;

- Provinciewet;
- Wet Poortwachter;
- Archiefwet;
- APPA;
- Arbeidstijdenwet;
- Pensioenwet;
- Wet verbreding Poortwachter;
- WIA;
- WW en
- Wet op de loonbelasting.

Zijn er normen van toepassing op de gegevensverwerking?

De gegevensverwerking is lijn met de

- (ISO27001);
- BIO (ISO27002);
- NEN2082.

Evaluatie : Aanvaardbaar

Evaluatie commentaar :

opmerkingen aangepast

Gegevens, processen en de levenscyclus ondersteunende systemen

Welke persoonsgegevens worden verwerkt?

Vanuit de rol als Gegevensverantwoordelijke/verwerker bevat de gegevensverwerking gegevens van personeelsleden van Provincie Limburg en Provinciale Staten

Vanuit de rol als gegevensverwerker bevat de gegevensverwerking de gegevens van personeelsleden van RUD-Zuid Limburg, Bonnefantenmuseum en de Zuid Limburgse Stoom Maatschappij (ZLSM).

Het betreft de volgende gegevens:

- NAW;
- bankrekening;
- dienstverband;
- verzuim;
- lid personeelsvereniging;
- declaratiegegevens;
- sollicitaties;
- beoordelingen;
- CV;
- Geboortedatum + -plaats;
- Geslacht;
- Telefoonnummer en e-mailadres (zakelijk en/of prive);
- Titulatuur;
- VOG;
- Integriteitsverklaring;
- Datum ingang en einde inhuur;
- Omvang aanstelling;
- Werkrooster;
- Historische arbeidsrelatie;
- Personeelsnummer;
- Vervoerskeuze;
- Salaris (Salarisinschaling, Salaris toelages/inhoudingen permanent en incidenteel);
- Loonbelastingverklaring/loonheffingsgegevens;
- Loonbeslag;
- Speciale aanduidingen belastingdienst (bijv. auto van de zaak);
- Notities;
- Aanmelding pensioen;
- Pensioendatum (AOW-datum);
- Deelname IPAP-verzekering;
- Begindatum en einddatum arbeidsongeschiktheid;
- Percentage arbeidsongeschiktheid;
- Burgerlijke staat + datum burgerlijke staat;
- Naam en geboortedatum partner (noodzakelijk tbv pensioenregeling);
- Naam en geboortedatum kinderen (aanvragen ouderschaps en aanvullend geboorte verlof) en
- Arbeidsverleden
- Nationaliteit.

Welke bijzondere persoonsgegevens worden verwerkt?

Binnen de gegevensverwerking worden de volgende bijzonder persoonsgegevens verwerkt:

- declaratie IKB vwb vakbondscontributie;
- financiële gegevens (zoals loonbeslag);
- verklaring omtrent gedrag (VOG);
- kopie identiteitsbewijs;
- nationaliteit en
- politiek lidmaatschap (statenleden).

Hoe werkt de levenscyclus van persoonsgegevens en processen?

De levenscyclus van de (actieve)persoonsgegevens loopt parallel aan het dienstverband van de betreffende medewerker.

Voorafgaand aan het dienstverband is sprake van werving en selectie. De gegevens van de aangenomen en afgewezen kandidaten worden gearchiveerd/vernietigd conform de eisen uit de archiefwet vastgelegd in de selectielijst voor archiefbescheiden van de provinciale organen (PROVISA).

Na het dienstverband worden de gegevens in de dossiers na 10 jaar vernietigd m.u.v. de persoonsdossiers van de CDK, Gedeputeerden, Griffier en directeurs . Deze komen voor blijvende bewaring in aanmerking.

Evaluatie : Aanvaardbaar
Evaluatie commentaar :
Opmerkingen aangepast

Beschrijf de systemen, technieken en methoden voor gegevensverwerking.

Wat zijn de persoonsgegevens ondersteunende systemen?

E-Hrm bestaat uit een viertal systemen, [REDACTED], [REDACTED] [REDACTED] en de p [REDACTED] De systemen worden afgenomen als [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Welke technieken en methoden worden gebruikt voor de gegevensverwerking?

De persoonsgegevens worden verwerkt door gebruik te maken van de functionaliteiten van de betreffende systemen. Dit betreft voornamelijk handmatige invoer van gegevens. Automatische verwerking heeft betrekking op de salarisadministratie, saldi (verlof, ikb etc.)

Op basis van de opgenomen gegevens kunnen management-rapportages (PDF) worden gemaakt (dashboard). Op basis hiervan kunnen analyses (Excel) worden uitgevoerd.

Er wordt geen gebruik gemaakt van algortimes (semi- geautomatische besluitvorming, profilering, bigdata verwerkingen).

Evaluatie : Aanvaardbaar
Evaluatie commentaar :
Opmerkingen aangepast

Fundamentele principes

Evenredigheid en noodzaak

Zijn de verwerkingsdoeleinden gespecificeerd, expliciet en legitiem?

Ja, voor de uitvoering van een HRM-proces dat voldoet aan de wettelijke verplichtingen wordt gebruik gemaakt van een geautomatiseerde toepassing.
Zie ook de vraag "Wat zijn de doeleinden van de gegevensverwerkingen?"

Evaluatie : Aanvaardbaar

Wat is de wettelijke basis om de gegevensverwerking rechtmatig te maken?

De gegevens verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting. Daarnaast worden additionele gegevens verwerkt die noodzakelijk zijn voor het uitvoeren van een overeenkomst.

Zie ook: Welke wet en regelgeving hebben betrekking op de gegevensverwerkingen?

Evaluatie : Aanvaardbaar

Zijn de persoonsgegevens adequaat, relevant en beperkt tot wat nodig is met betrekking tot de doeleinden waarvoor ze worden verwerkt ('gegevensminimalisatie')?

Er worden enkel die gegevens opgenomen die betrekking hebben op de wettelijke verplichting of uit hoofde van de overeenkomst (interne bedrijfsvoering) noodzakelijk zijn. Eventuele overige gegevens kunnen door de medewerker zelf worden aangevuld op basis van vrijwilligheid (b.v. partnerregistratie).

Evaluatie : Aanvaardbaar

Zijn de persoonsgegevens juist en worden ze up-to-date gehouden?

Ja, de persoonsgegevens worden door de medewerker zelf up-to-date gehouden daarnaast worden de standaardgegevens ten aanzien van functie en salaris geactualiseerd door management en medewerkers van Personeel en Organisatie.

Evaluatie : Aanvaardbaar

Wat is de bewaartermijn van de persoonsgegevens?

Voorafgaand aan het dienstverband is sprake van werving en selectie. De gegevens van afgewezen kandidaten worden gearchiveerd/vernietigd conform de eisen uit de archiefwet vastgelegd in de selectielijst voor archiefbescheiden van de provinciale organen (PROVISA). Voor de gegevens van afgewezen kandidaten geldt een bewaartermijn (indien toestemming hiervoor is gegeven) van maximaal 1 jaar. Anders geldt een termijn van 4 weken. Voor een uitgevoerd assessment geldt een bewaartermijn van 1 jaar.

De gegevens van de aangenomen kandidaat worden opgenomen binnen het systeem. Ook deze worden gearchiveerd/vernietigd conform de eisen uit de archiefwet vastgelegd in de selectielijst voor archiefbescheiden van de provinciale organen (PROVISA). Na het dienstverband worden de gegevens in de dossiers na 10 jaar vernietigd m.u.v. de persoonsdossiers van de CDK, Gedeputeerden, Griffier en directeurs . Deze komen voor blijvende bewaring in aanmerking.

De gegevens van de aangenomen kandidaat zoals persoonsgegevens, getuigschrift, loonbelastingverklaring, arbeidsovereenkomst en wijzigingen, correspondentie benoemingen, eed/beloofte, promotie en demotie, detachering, correspondentie ontslag worden 10 jaar na uit dienst bewaard.

Gegevens over diploma's en opleidingen die tijdens in dienst zijn behaald, verslagen van functioneringsgesprekken, salarisafspraken, salarisadministratie, gratificaties en incidentele beloningen, levensloop, verlof(opname) roosterwijzigingen en verlofwijzigingen hebben een bewaartermijn van 10 jaar.

Voor loonbeslag geldt een bewaartermijn van 7 jaar na afwikkeling.

Gegevens over verzuim, verslagen omtrent Wet Verbetering Poortwachter, correspondentie over ziekte van UWV en bedrijfsarts worden bewaard tot 10 jaar na uit dienst. Dit zelfde geldt voor verslagen van financiële problemen en verslagen rondom probleemsituaties. Voor een psychologisch onderzoek geldt een bewaartermijn van 1 jaar na het vervallen van het belang ervan.

Als er sprake is van een arbeidsconflict of er een rechtszaak loopt dan worden betreffende gegevens zo lang bewaard als nodig is.

 Onderscheid wordt bepaald op basis van kenmerken.

Evaluatie : Verbeterbaar
Actieplan / corrigerende maatregelen :

Evaluatie commentaar :

Hoe geregeld wordt dat betrokkenen hun persoonlijke rechten kunnen uitoefenen.

Hoe worden de betrokkenen geïnformeerd over de gegevensverwerking?

De betrokkenen worden geïnformeerd bij het eerste contact met de werkgever. In principe is dit voorafgaand/tijdens het werving en selectie proces.

Evaluatie : Aanvaardbaar

Hoe wordt de toestemming van betrokkenen verkregen?

Voor het grootste deel valt de gegevensverwerking onder de grondslag "wettelijke verplichting" en "uit hoofde van een overeenkomst". Verder kan de medewerker zelf gegevens toevoegen op basis van vrijwilligheid (impliciete toestemming).

Toestemming wordt verkregen voor het opslaan van de sollicitatiegegevens tot maximaal 1 jaar.

Evaluatie : Aanvaardbaar

Hoe kunnen betrokkenen hun recht op toegang en overdraagbaarheid van persoonsgegevens uitoefenen?

Dit kan via een aanvraag bij het cluster P&O.
Zie handleiding AVG: rechten van betrokkenen.

Aandachtspunt: Procedure dient nog te worden uitgewerkt.

Evaluatie : Aanvaardbaar

Hoe kunnen betrokkenen hun recht op rectificatie en verwijdering uitoefenen?

Dit kan via een aanvraag bij het cluster P&O. Verder kan een deel van de gegevens door de medewerker zelf worden bijgehouden.
Zie handleiding AVG: rechten van betrokkenen.

Evaluatie : Aanvaardbaar

Hoe kunnen betrokkenen hun recht op beperking uitoefenen en bezwaar maken?

Dit kan via een aanvraag bij het cluster P&O.
Zie handleiding AVG: rechten van betrokkenen.

Aandachtspunt: Procedure dient nog te worden uitgewerkt.

Evaluatie : Aanvaardbaar

Zijn de verplichtingen van de verwerkers duidelijk geïdentificeerd en geregeld in een (verwerkers)overeenkomst?

Ja, zie verwerkersovereenkomst.

Evaluatie : Verbeterbaar

Actieplan / corrigerende maatregelen :

Zijn de persoonsgegevens in het geval van gegevensoverdracht buiten de Europese Unie voldoende beschermd?

De gegevens worden verwerkt binnen de EER.

Evaluatie : Aanvaardbaar

Geplande of bestaande maatregelen

6.1.2 Scheiding van taken

Algemeen:
De scheiding van taken wordt vertaald naar rollen. Aan een rol worden rechten toegekend voor toegang tot en bepaalde handelingen, binnen een toepassing (role-based acces). Een rol wordt vertaald naar 'n groep binnen het [redacted]

Specifiek:
Binnen [redacted] worden rollen gedefinieerd en gekoppeld aan personen. Rollen geven toegang tot workflows, modules, tabbladen, pagina's ed. Autorisatie voor de [redacted] en [redacted] wordt geregeld op basis van [redacted]

Aandachtspunt:
Binnen [redacted] vindt autorisatie plaats op individueel niveau in plaats van op groepsniveau.

Evaluatie : Aanvaardbaar
Evaluatie commentaar :
[redacted]
[redacted]

6.2.2 Telewerkbeleid

Algemeen:
Standaard worden de toepassingen van Provincie Limburg via de [redacted] omgeving beschikbaar gesteld. [redacted]
[redacted]

Specifiek:
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]

Aandachtspunt:
[redacted]
[redacted]

Evaluatie : Verbeterbaar
Actieplan / corrigerende maatregelen :
[redacted]
Evaluatie commentaar :
[redacted]
[redacted]
[redacted]

7.1.1 Screening personeel

Algemeen:
Voor nieuwe medewerkers die in dienst komen bij Provincie Limburg dient een voor de functie verstrekte verklaring omtrent gedrag overlegd te worden.

Specifiek:
n.v.t.

Aandachtspunt:
n.v.t.

Evaluatie : Aanvaardbaar

7.1.2 Beveiliging in arbeidsvoorwaarden

Algemeen:
Interne medewerkers worden tijdens het introductieprogramma geïnformeerd over informatieveiligheid. Daarnaast krijgen nieuwe medewerkers informatie over het omgaan met bedrijfsmiddelen zoals bijvoorbeeld, digitale werkplek, smartphone ed.

Het omgaan met informatie, geheimhouding en integriteit wordt geadresseerd tijdens het afleggen van de eed/belofte.
De Ambtenarenwet (2017) bevat oa. artikelen met betrekking tot geheimhouding/ beschikbaar stellen van informatie (art. xx.x)

Specifiek:
n.v.t.

Aandachtspunt:
n.v.t.

Evaluatie : Aanvaardbaar

8.2.1 Classificatie van informatie

Algemeen:
Gegevens dienen geclassificeerd te worden (openbaar, bedrijfsvertrouwelijk, vertrouwelijk en geheim). Op basis van deze classificatie kunnen aanvullende maatregelen genomen worden.

Specifiek:
[Redacted]
[Redacted]

Aandachtspunt:
[Redacted]

Evaluatie : Verbeterbaar

Actieplan / corrigerende maatregelen :

[Redacted]
[Redacted]
[Redacted]
[Redacted]

8.2.2 Informatie labels

Algemeen:
[Redacted]
[Redacted]

Specifiek:
n.v.t.

Aandachtspunt:
n.v.t.

Evaluatie : Aanvaardbaar

8.2.3 Procedures voor behandelen van bedrijfsmiddelen

Algemeen:
Op basis van het classificatie schema en de labeling van de gegevens dient duidelijk gemaakt te worden welke behandeling en opslag van gegevens wordt vereist.

Specifiek:
[Redacted]
[Redacted]
[Redacted]
[Redacted]

Aandachtspunt:
[Redacted]

Evaluatie : Verbeterbaar

Actieplan / corrigerende maatregelen :

[Redacted]
[Redacted]
[Redacted]

8.3.1 Beheer van verwijderbare media

Algemeen:
Informatie op verwijderbare media wordt overeenkomstig het classificatieschema behandeld. Op de herbruikbare media die de organisatie verlaten staan alleen de noodzakelijke gegevens.

Specifiek:
Afspraken zijn gemaakt met [Redacted] (verwerkersovereenkomst)

Aandachtspunt:
n.v.t.

Evaluatie : Aanvaardbaar

8.3.2 Procedures voor verwijderen van media

Algemeen:
[Redacted]

Specifiek:
A [Redacted]

Aandachtspunt:
n.v.t.

Evaluatie : Aanvaardbaar

8.3.3 Bescherming media bij fysiek overdragen

Algemeen:
[Redacted]

Specifiek:
n.v.t.

Aandachtspunt:
[Redacted]
[Redacted]

Evaluatie : Verbeterbaar

Actieplan / corrigerende maatregelen :

[Redacted]

9.1.1 Beleid voor toegangsbeveiliging

Algemeen:

Toegang tot informatie wordt geregeld via [Redacted]

Specifiek:

[Redacted]

Aandachtspunt:

[Redacted]

Evaluatie : Verbeterbaar

Actieplan / corrigerende maatregelen :

[Redacted]

9.1.2 Alleen bevoegde toegang tot netwerken en netwerkdiensten

Algemeen:

[Redacted]

Specifiek:

[Redacted]

Aandachtspunt:

[Redacted]

Evaluatie : Verbeterbaar

Actieplan / corrigerende maatregelen :

[Redacted]

9.2.1 Registratie en afmelden van gebruikers

Algemeen:

[Redacted]

Specifiek:

[Redacted]

Aandachtspunt:

[Redacted]

Evaluatie : Verbeterbaar

Actieplan / corrigerende maatregelen :

[Redacted]

9.2.2 Procedure voor toegang verlenen gebruikers

Algemeen:

[Redacted]

Specifiek:

[Redacted]

Aandachtspunt:

[Redacted]

Evaluatie : Aanvaardbaar

Evaluatie commentaar :

[Redacted]

9.2.6 Toegangsrechten intrekken of aanpassen bij beëindigen werkzaamheden

Algemeen:

[Redacted]

Specifiek:

zie 9.2.2

Aandachtspunt:

zie 9.2.2

Evaluatie : Aanvaardbaar

Evaluatie commentaar :

zie 9.2.2.

9.3.1 Geheime authenticatie-informatie gebruiken

Algemeen:

[Redacted]

Specifiek:

[Redacted]

Aandachtspunt:

[Redacted]

Evaluatie : Aanvaardbaar

Evaluatie commentaar :

[Redacted]

9.4.1 Beperking toegang tot informatie

Algemeen:

[Redacted]

Specifiek:

zie 9.2.2.

Aandachtspunt:

zie 9.2.2.

Evaluatie : Aanvaardbaar

Evaluatie commentaar :

zie 9.2.2.

9.4.2 Beveiligde inlogprocedures

Algemeen:

[Redacted]

Specifiek:

[Redacted]

Aandachtspunt:

[Redacted]

Evaluatie : Verbeterbaar

Actieplan / corrigerende maatregelen :

[Redacted]

9.4.3 Systeem voor wachtwoordbeheer

Algemeen:

[Redacted]

Specifiek:

n.v.t.

Aandachtspunt:
n.v.t.

Evaluatie : Aanvaardbaar

9.4.4 Maatregelen gebruik speciale systeemhulpmiddelen

Algemeen:

[Redacted]

Specifiek:

N.v.t.

Aandachtspunt:

[Redacted] n)

Evaluatie : Aanvaardbaar

9.4.5 Toegangsbeveiliging op programmabroncode

Algemeen:

[Redacted]

[Redacted]

Specifiek:

[Redacted]

Aandachtspunt:

[Redacted]

[Redacted]

Evaluatie : Verbeterbaar

Actieplan / corrigerende maatregelen :

[Redacted]

[Redacted]

10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen

Algemeen:

[Redacted]

[Redacted]

Specifiek:

[Redacted]

Aandachtspunt:

[Redacted]

Evaluatie : Aanvaardbaar

Evaluatie commentaar :

[Redacted]

[Redacted]

[Redacted]

10.1.2 Sleutelbeheer

Algemeen:

[Redacted]

Specifiek:

n.v.t.

Aandachtspunt:

[Redacted]

Evaluatie : Aanvaardbaar

Evaluatie commentaar :

S [Redacted]

[Redacted]

11.1.1 Gebruik fysieke beveiligingszones

Algemeen:

[Redacted]

Specifiek:

[Redacted]

Aandachtspunt:

n.v.t.

Evaluatie : Aanvaardbaar

11.1.5 Werken in beveiligde gebieden

Algemeen:

Specifiek:

Aandachtspunt:
n.v.t.

Evaluatie : Aanvaardbaar

11.1.6 Beheersing Laad- en loslocaties

Algemeen:

Specifiek:

n.v.t.

Aandachtspunt:

Evaluatie : Aanvaardbaar

Evaluatie commentaar :

11.2.6 Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein

Algemeen:

Specifiek:

zie 6.2.2.

Aandachtspunt:

zie 6.2.2.

Evaluatie : Aanvaardbaar

Evaluatie commentaar :

zie 6.2.2.

11.2.7 Veilig verwijderen of hergebruiken van apparatuur

Algemeen:

Specifiek:

Aandachtspunt:

Evaluatie : Aanvaardbaar

Evaluatie commentaar :

Zie ook 8.2.1. en afspraken met █████ (verwerkersovereenkomst)

11.2.8 Bescherming onbeheerde gebruikersapparatuur

Algemeen:

Binnen de Provincie Limburg geldt een clear desk en clear screen policy. Bij verlaten van de werkplek dient het scherm te worden afgesloten. In het algemeen is een █████ aanwezig (tijdsperiode?).

Specifiek:

Aandachtspunt:

Evaluatie : Verbeterbaar

Actieplan / corrigerende maatregelen :

11.2.9 ‘Clear desk’- en ‘clear screen’-beleid

Algemeen:

Indien de werkplek niet wordt gebruikt (verlaten) wordt de werkplek vergrendeld (zie ook 11.2.8). Het cleardesk beleid houdt in dat er geen vertrouwelijke documenten op de onbeheerde bureaus aanwezig zijn.

Specifiek:

Aandachtspunt:

Evaluatie : Aanvaardbaar

Evaluatie commentaar :

12.4.2 Beschermen van informatie in logbestanden

Algemeen:

Specifiek:

Aandachtspunt:

Evaluatie : Verbeterbaar

Actieplan / corrigerende maatregelen :

13.2.1 Beleid en procedures voor informatietransport

Algemeen:

Met betrekking tot informatietransport zijn algemene afspraken gemaakt.

Specifiek:

Aandachtspunt:

Evaluatie : Verbeterbaar

Actieplan / corrigerende maatregelen :

13.2.2 Overeenkomsten over informatietransport

Algemeen:

Het uitwisselen van informatie tussen de organisatie en derden en derden onderling dient opgenomen te zijn in de overeenkomst met de betreffende derden. Ingeval van persoonsgegevens is dit opgenomen in de verwerkersovereenkomst.

Specifiek:

Met [REDACTED] is een verwerkersovereenkomst afgesloten.

Aandachtspunt:

Evaluatie : Aanvaardbaar

Evaluatie commentaar :

13.2.3 Bescherming elektronische berichten

Algemeen:

Informatie in elektronische berichten dient passend te zijn beveiligd.

Specifiek:

Met [REDACTED] is een verwerkersovereenkomst afgesloten.

Aandachtspunt:

Evaluatie : Verbeterbaar

Actieplan / corrigerende maatregelen :

13.2.4 Vertrouwelijkheids- of geheimhoudingsovereenkomst

Algemeen:

Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen, behoren te worden vastgesteld, regelmatig te worden beoordeeld en gedocumenteerd.

Specifiek:

[Redacted]

Aandachtspunt:

[Redacted]

Evaluatie : Aanvaardbaar

Evaluatie commentaar :

[Redacted]

14.1.2 Toepassingen op openbare netwerken beveiligen

Algemeen:

Informatie die deel uitmaakt van uitvoeringsdiensten en die via openbare netwerken wordt uitgewisseld, behoort te worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegd openbaarmaking en wijziging.

Specifiek:

[Redacted]

Aandachtspunt:

[Redacted]

Evaluatie : Aanvaardbaar

Evaluatie commentaar :

[Redacted]

14.1.3 Transacties van toepassingen beschermen

Algemeen:

Informatie die deel uitmaakt van transacties van toepassingen behoort te worden beschermd ter voorkoming van onvolledige overdracht, foutieve routing, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.

Specifiek:

[Redacted]

Aandachtspunt:

[Redacted]

Evaluatie : Verbeterbaar

Actieplan / corrigerende maatregelen :

[Redacted]

18.1.4 Borging van privacy en bescherming van persoonsgegevens

Algemeen:

Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.

[Redacted]

Aandachtspunt:

n.v.t.

Evaluatie : Aanvaardbaar

18.1.5 Voorschriften voor het gebruik van cryptografische beheersmaatregelen

Algemeen:

Cryptografische beheersmaatregelen behoren te worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving. Zie ook pas-toe-leg-uit lijst van het Forum voor standaardisatie.

Specifiek:

zie 10.1.1.

Aandachtspunt:

zie 10.1.1.

Onrechtmatige toegang tot persoonsgegevens

Wat kunnen de belangrijkste gevolgen voor de betrokkenen zijn als het risico zou optreden?

Wat zijn de belangrijkste dreigingen die tot het risico kunnen leiden?

Wat zijn de risicobronnen?

Welke van de geïdentificeerde maatregelen dragen bij aan het mitigeren van het risico?

Hoe schat u de ernst van het risico, rekening houdend met de potentiële effecten en geplande maatregelen?

Hoe schat u de waarschijnlijkheid van het risico, vooral met betrekking tot dreigingen, risicobronnen en geplande maatregelen?

Evaluatie : Verbeterbaar

Actieplan / corrigerende maatregelen :

Ongewenste wijziging van persoonsgegevens

Wat kunnen de belangrijkste gevolgen voor de betrokkenen zijn als het risico zou optreden?

Wat zijn de belangrijkste dreigingen die tot het risico kunnen leiden?

Wat zijn de risicobronnen?

Welke van de geïdentificeerde maatregelen dragen bij aan het mitigeren van het risico?

Hoe schat u de ernst van het risico, met name op basis van de potentiële effecten en geplande maatregelen?

Hoe schat u de waarschijnlijkheid van het risico, vooral met betrekking tot dreigingen, risicobronnen en geplande maatregelen?

Evaluatie : Verbeterbaar

Actieplan / corrigerende maatregelen :

[Redacted]

Verdwijnen van persoonsgegevens

Wat kunnen de belangrijkste gevolgen voor de betrokkenen zijn als het risico zou optreden?

[Redacted]

Wat zijn de belangrijkste dreigingen die tot het risico kunnen leiden?

[Redacted]

Wat zijn de risicobronnen?

[Redacted]

Welke van de geïdentificeerde maatregelen dragen bij aan het mitigeren van het risico?

[Redacted]

Hoe schat u de ernst van het risico, met name op basis van de potentiële effecten en geplande maatregelen?

[Redacted]

Hoe schat u de waarschijnlijkheid van het risico, vooral met betrekking tot dreigingen, risicobronnen en geplande maatregelen?

[Redacted]

Evaluatie : Verbeterbaar

Actieplan / corrigerende maatregelen :

[Redacted]

Overzicht

Fundamentele principes	Geplande of bestaande maatregelen
Doelbinding	
Rechtsgrondslag	
Adequate persoonsgegevens	
Gegevens nauwkeurigheid	
Bewaartermijn	
Informatie voor de betrokkenen	
Verkrijgen van toestemming	
Recht op toegang en gegevensportabiliteit	
Recht op rectificatie en verwijdering	
Recht op beperking en bezwaar	
Verwerkers	
Overdrachten	

Risico's

- Onrechtmatige toegang tot
persoonsgegevens
- Ongewenste wijziging van
persoonsgegevens
- Verdwijnen van
persoonsgegevens

Verbeterbare Maatregelen
Aanvaardbare Maatregelen

Fundamentele principes

Bewaartermijn

Actieplan / corrigerende maatregelen :

Evaluatie commentaar :

Verwachte datum van implementatie : 01/06/2021

Verwerkers

Actieplan / corrigerende maatregelen :

Verwachte datum van implementatie : 01/09/2021

6.2.2 Telewerkbeleid

Actieplan / corrigerende maatregelen :

Evaluatie commentaar :

8.2.1 Classificatie van informatie

Actieplan / corrigerende maatregelen :

8.2.3 Procedures voor behandelen van bedrijfsmiddelen

Actieplan / corrigerende maatregelen :

8.3.3 Bescherming media bij fysiek overdragen

Actieplan / corrigerende maatregelen :

9.1.1 Beleid voor toegangsbeveiliging

Actieplan / corrigerende maatregelen :

9.1.2 Alleen bevoegde toegang tot netwerken en netwerkdiensten

Actieplan / corrigerende maatregelen :

9.2.1 Registratie en afmelden van gebruikers

Actieplan / corrigerende maatregelen :

9.4.2 Beveiligde inlogprocedures

Actieplan / corrigerende maatregelen :

9.4.5 Toegangsbeveiliging op programmabroncode

Actieplan / corrigerende maatregelen :

11.2.8 Bescherming onbeheerde gebruikersapparatuur

Actieplan / corrigerende maatregelen :

12.4.2 Beschermen van informatie in logbestanden

Actieplan / corrigerende maatregelen :

13.2.1 Beleid en procedures voor informatietransport

Actieplan / corrigerende maatregelen :

[Redacted text]

13.2.3 Bescherming elektronische berichten

Actieplan / corrigerende maatregelen :

[Redacted text]

14.1.3 Transacties van toepassingen beschermen

Actieplan / corrigerende maatregelen :

[Redacted text]

[illegible]

Actieplan / corrigerende maatregelen :

[Redacted]

[Redacted]

[Redacted]

Actieplan / corrigerende maatregelen :

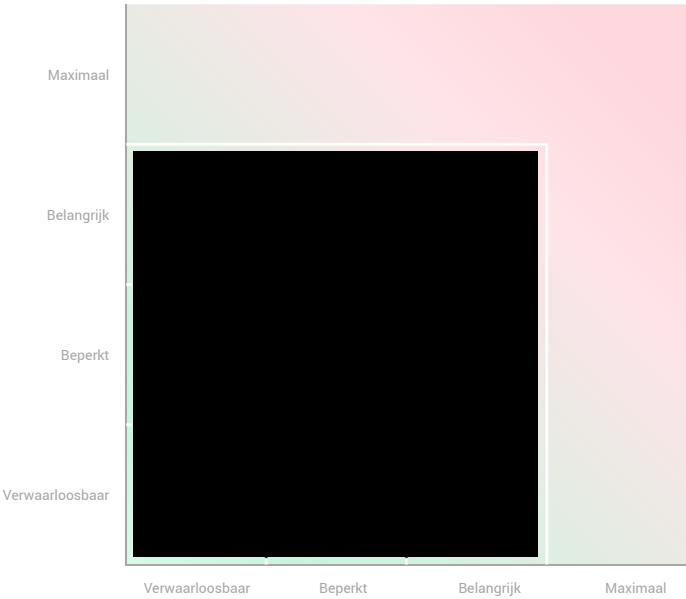
[Redacted]

[Redacted]

[Redacted]



Risico omvang



Risico waarschijnlijkheid

- Geplande of bestaande maatregelen
- Met de geïmplementeerde corrigerende maatregelen
- (I)Onrechtmatige toegang tot persoonsgegevens
- (U)Ongewenste wijziging van persoonsgegevens
- ((D)Verdwijnen van persoonsgegevens