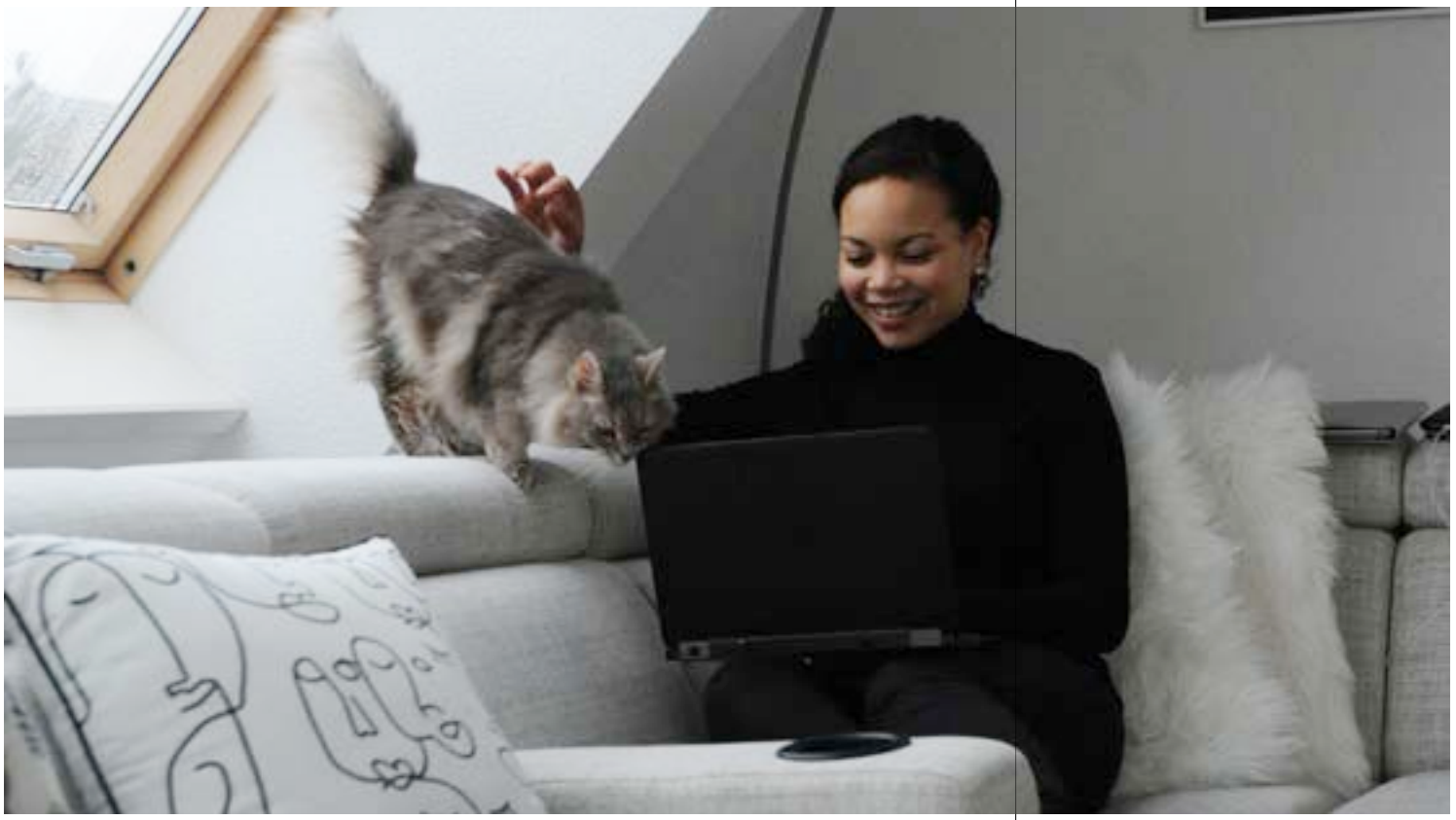
Ministerie van Economische Zaken
en Klimaat

INFORMATIEBEVEILIGING EN PRIVACY

Gids voor leveranciers met informatie over:

- wat wij van u verwachten als leverancier
- de aanpak voor informatie-beveiliging en privacy van EZK



Het beveiligen van informatie en beschermen van persoonsgegevens heeft voor het ministerie van Economische Zaken en Klimaat (EZK) de hoogste prioriteit. Dat vraagt om een grote inspanning van onze eigen medewerkers, maar zeker ook van onze leveranciers. In deze beknopte gids leest u er meer over.

EZK zet zich in voor een veilige organisatie die de belangen en rechten van onze burgers en de samenleving waarborgt. Dit vragen we van onze medewerkers, onze organisaties en ook van onze leveranciers. Deze gids omschrijft beknopt het informatiebeveiligings- en privacybeleid van EZK. Wij verwachten dat u zich als leverancier houdt aan dezelfde principes als wij. Alleen dan kunnen we realiseren dat de informatiebeveiliging en privacy in de hele keten gewaarborgd wordt. Overige specifieke eisen voor informatiebeveiliging en privacy vindt u in de onderlinge overeenkomst.

Visie Informatiebeveiliging

EZK staat voor een toekomst waarin onze doelstellingen optimaal bereikt worden in een veilige en betrouwbare omgeving. Deze omgeving geeft ruimte aan nieuwe technologische ontwikkelingen en faciliteert innovatieve toepassingen. Deze toekomst creëren we door onze informatiebeveiliging slim in te zetten en mee te laten groeien. Zo realiseren we de beveiliging van informatie bij de bron, een robuuste toegangsbeveiliging en een infrastructuur die nieuwe technologische toepassingen mogelijk maakt. De informatiebeveiligingsorganisatie ondersteunt de organisatie hierbij door een actueel inzicht te bieden in haar kansen en dreigingen.

Doelstelling is adequate bescherming van de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening én zorgvuldige omgang met persoonsgegevens

Visie Privacy

Gegevens van en over burgers moeten bij EZK veilig zijn en hun privacy moet zijn gewaarborgd. Dat betekent dat EZK duurzaam en vertrouwd omgaat met (persoons)gegevens. Los van het voldoen aan wet- en regelgeving, wil EZK een betrouwbare partner zijn waar persoonsgegevens veilig en verantwoord worden verwerkt bij de uitvoering en het waarborgen van hun publieke taak.
De doelstelling van EZK Informatiebeveiliging en privacy is: op basis van risicomanagement te zorgen voor een adequate bescherming van de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie(voorziening), teneinde de continuïteit van de bedrijfsprocessen en het vertrouwen in het ministerie door burgers, bedrijfsleven en andere overheden te beschermen.

Regelgeving
Wij zien erop toe dat er in ieder geval conform de volgende wetgeving en normenkaders wordt gehandeld:

- Baseline Informatiebeveiliging Overheid (BIO)
- De Algemene Verordening Gegevensbescherming (AVG)
- ISO standaard 31000 (Risk management)
- ISO 27001
- ISO 27002
- Voorschrift Informatiebeveiliging Rijksdienst 2007 (VIR 2007)
- Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie 2013 (VIR-BI 2013)

Sturing en verantwoording EZK
EZK heeft haar sturing en toezicht ingericht middels de volgende instrumenten.

- Kwaliteitscyclus is ingevoerd op informatiebeveiliging en privacy.
- De ministeries worden getoetst door de Algemene Rekenkamer (ARK) en de Audit Dienst Rijk (ADR).
- Toetsingen vinden plaats op onze systemen, processen, medewerkers en leveranciers door onafhankelijke partijen, om blijvend de veiligheid en gegevensbescherming te kunnen waarborgen.

Organisatorische maatregelen
EZK zet verschillende organisatorische maatregelen in om beveiliging en privacy te waarborgen. Hieronder treft u een aantal voorbeelden aan.

De nationale veiligheid en beveiliging van gegevens en ICT staan voorop

- Informatiebeveiliging maakt onderdeel uit van het integrale beveiligingsbeleid van de Beveiligingsambtenaar (BVA).
- Medewerkers en externen krijgen enkel toegang tot informatie-(systemen) na autorisatie door de daartoe bevoegde persoon of instantie.
- We gaan uit van het 'need to know' principe en bewustwording bij geautoriseerde personen op de onderwerpen informatiebeveiliging en privacy.
- Wij sturen op Privacy by Design en Security by Design.
- De nationale veiligheid van de Nederlandse samenleving, de beveiliging van gegevens en Informatie- en Communicatietechnologie (ICT) en de privacy van onze burgers en medewerkers staan voorop.
- Om vroegtijdig privacy risico's voor de organisatie in kaart te brengen wordt de Privacy Impact Assessment (PIA) ingezet.
- Gebruik voor de toegang tot digitale systemen sterke wachtwoorden, tweefactorauthenticatie en wachtwoordmanagers.

Het benutten van kansen, zoals de inzet van nieuwe technologieën, valt samen met het nemen van risico's. Het is belangrijk om de juiste balans hierin te vinden. Risicomanagement is een continu proces waarbij risico's worden geïdentificeerd en de mogelijke impact wordt bepaald. Door risico's op gestructureerde wijze in kaart te brengen en risicobeperkende maatregelen te nemen, zorgen wij gezamenlijk voor de veiligheid van gegevens en systemen.

Wij vragen van u dezelfde maatregelen en principes te hanteren als omschreven in deze gids. Zo kunnen we samen de veiligheid en privacy van de gegevens en processen waarborgen. Wij verwerken alleen persoonsgegevens als hiervoor een rechtmatige grondslag aanwezig is. Wij stellen de betrokkene centraal. De persoonsgegevens worden niet langer bewaard dan strikt noodzakelijk voor het doel van de verwerking. Houd uw persoonsgegevens juist en actueel en wees terughoudend met het verstrekken van gegevens aan derden. ■

Heeft u nog vragen?
Als u nog vragen heeft op het gebied van informatiebeveiliging en/of privacy over bijvoorbeeld procedures of nadere invulling van maatregelen, dan kunt u dat altijd kenbaar maken aan uw contactpersoon binnen EZK. Ook vindt u meer informatie over specifieke eisen in het contract of de overeenkomst.

Nadere toelichting

Samen sterk: Informatiebeveiliging en privacy EZK

Het ministerie van Economische Zaken en Klimaat (EZK) hecht grote waarde aan publiek-private samenwerking waarbij het rijk en bedrijven samenwerken om economische en maatschappelijke kansen te benutten, zoals een CO2-neutrale samenleving, sterke digitale economie en de omschakeling naar kringlooplandbouw. EZK heeft de ambitie om vooruitstrevende en efficiënte informatie- en communicatiemiddelen in te zetten zodat taken en verantwoordelijkheden, zoals het optimaliseren van de ondersteuning aan burgers en het bedrijfsleven, gerealiseerd kunnen worden. Informatiebeveiliging en privacy zijn daarbij van onmisbaar belang.

Beschermen van belangen

De te beschermen belangen zoals bedrijfsgeheimen, persoonsgegevens, geclassificeerde of **gerubriceerde informatie** en het waarborgen van continuïteit hebben voor het ministerie de hoogste prioriteit. Dat vraagt om een grote inspanning van onze eigen medewerkers, maar zeker ook van onze samenwerkingspartners. Niet of onvoldoende beveiligde gegevens en uitval van informatie- en communicatietechnologie (ICT) zorgen voor een onacceptabel risico op reputatieschade, financiële schade of het verlies van waardevolle data. Dit betekent dat EZK en haar samenwerkingspartners, om het vertrouwen van de burger in het openbaar bestuur te behouden, maatregelen moeten nemen om de veiligheid van gegevens te garanderen.

Wetgeving, normenkader en maatregelen

De overheid werkt met de Baseline Informatie Beveiliging Overheid (BIO). Dit is het **normenkader** voor informatiebeveiliging binnen de gehele overheid, gebaseerd op de internationaal erkende en actuele ISO-normatiek (**ISO 27001**). De implementatierichtlijnen zijn niet in de BIO opgenomen, hiervoor wordt verwezen naar de ISO 27002. Er zijn drie cruciale aspecten om het beoogde niveau van beveiliging van gegevens, informatiesystemen en bedrijfsprocessen te realiseren. Voor elk aspect wordt beoordeeld hoe belangrijk het is. Hoe hoger de inschatting van het belang is, hoe belangrijker het nemen van voldoende maatregelen is.

1. Beschikbaarheid, te garanderen door goed onderhoud en door systemen regelmatig te updaten. Back-ups en fallback scenario's zorgen ervoor dat bij verstoring men snel weer de beschikking kan hebben over de gegevens.
2. Integriteit, de juistheid en volledigheid gedurende de gehele levenscyclus van gegevens. Of gegevens nu onderweg zijn of opgeslagen, gegevens mogen niet gewijzigd worden door onbevoegden (toegangsbeheer op basis van "need to know").
3. Vertrouwelijkheid, die mede gaat over privacy. Het nemen van maatregelen om te voorkomen dat gegevens in verkeerde handen terecht komen, terwijl de juiste personen er wel bij moeten kunnen.

Voor de verwerking van persoonsgegevens, gegevens die te herleiden zijn naar een geïdentificeerde of identificeerbare natuurlijke persoon, zijn de Algemene verordening gegevensbescherming (**AVG**) en de Uitvoeringswet Algemene verordening gegevensbescherming (**UAVG**) van toepassing. Om daar op een goede wijze invulling aan te geven, heeft **EZK** een privacybeleid vastgesteld.
EZK blijft als verwerkingsverantwoordelijke altijd verantwoordelijk voor de verwerking van persoonsgegevens, maar ook aan samenwerkingspartners worden in de AVG eisen gesteld (**verwerker**). EZK past **Privacy by design en default** toe en vraagt dit ook van haar samenwerkingspartners. Zorgvuldige omgang met persoonsgegevens moet organisatorisch en technisch afgedwongen worden. De Rijksoverheid is transparant over de verwerking van haar persoonsgegevens. Het **AVG-register** biedt een overzicht van de typen gegevens die worden verwerkt, waarvoor deze gegevens zijn verzameld, wat er met de gegevens wordt gedaan en wie er verantwoordelijk is voor de verwerking.

Rollen en verantwoordelijkheden

Het vergroten van de weerbaarheid tegen mogelijke dreigingen of risico's is een doorlopend proces (plan, do, check, act) en begint met rollen en verantwoordelijkheden over en weer expliciet te bespreken. Het daadwerkelijk minimaliseren van risico's is de belangrijkste doelstelling. Het minimumniveau voor de beveiliging (ter illustratie: de **baselinetoets BBN BIO**) is afgesproken en helder vastgelegd. In een Service Level Agreement (SLA) zijn afspraken nader geconcretiseerd. Als een samenwerkingspartner namens EZK (verwerkingsverantwoordelijke) persoonsgegevens verwerkt, dan wordt door het ministerie waarvoor de verwerking wordt uitgevoerd een **verwerkersovereenkomst** opgesteld. In deze overeenkomst is bijvoorbeeld vastgelegd voor welke doeleinden gegevens verwerkt mogen worden, hoe gegevens beveiligd moeten worden en dat gegevens alleen gedeeld mogen worden binnen de vastgestelde doeleinden. Afwijkingen worden actief gerapporteerd en zijn onderdeel van een periodieke evaluatie. Prestaties zijn aantoonbaar en dienen als bewijs voor de contractueel overeengekomen (beveiligings)kwaliteit. Het nemen van preventieve aanvullende beveiligingsmaatregelen kan worden overeengekomen. Afspraken zijn gemaakt over het verstrekken van (bij voorkeur real-time) informatie over storingen en risico's van cybercrime. Dit zorgt ervoor dat er tijdig gereageerd kan worden op nieuw ontstane bedreigingen, risico's en incidenten. Een datalek bij een verwerker bijvoorbeeld dat waarschijnlijk een risico oplevert voor 'de rechten en vrijheden van betrokkenen' is meldingsplichtig. EZK moet dan als verwerkingsverantwoordelijke meteen (binnen 72 uur) een melding doen bij de Autoriteit Persoonsgegevens (AP). Leveranciers moeten hun keten van toeleveranciers bekendmaken en transparant zijn over de maatregelen die zij genomen hebben om de aan hen opgelegde eisen ook door te vertalen naar hun toeleveranciers. EZK heeft te allen tijde het recht toe te (laten) zien op de naleving (recht op audit) en samenwerkingspartners laten tenminste 1 keer per jaar een (interne of externe) audit uitvoeren voor de grootste risico's. ■

Dit is een uitgave van
Ministerie van Economische Zaken en Klimaat

Bezoekadres
Bezuidenhoutseweg 73
2594 AC Den Haag
Telefoonnummer: 070-379 8911

Postadres
Postbus 20401
2500 EK Den Haag

www.rijksoverheid.nl/ezk