Kennisnet

Informatiebeveiligings- en privacybeleid

Informatieverwerking binnen en namens Kennisnet

Versie 1.4 - 20 maart 2018

Laat ict werken **voor het onderwijs**

Voorwoord

Digitalisering in de maatschappij leidt tot toenemende beschikbaarheid van data en potentieel dus tot nieuwe of rijkere informatie. Dit biedt mogelijkheden om snellere en beter geïnformeerde keuzes maken. Facebook, LinkedIn, Twitter of gewoon via de email – iedereen is online. Zakelijke en publieke diensten springen daarop in door de consument op elk moment van de dag te bedienen met producten en informatie.

Digitalisering speelt ook een grote rol binnen het onderwijs, datasturing en informatisering maken het mogelijk om persoonlijk onderwijs te geven en leerlingen op “op maat” lesmateriaal en feedback aan te bieden. Iets dat in een klas van 25 kinderen zonder de inzet van ict praktisch onmogelijk is voor de docent. Tevens raken het onderwijsproces en het bedrijfsvoering proces hierdoor steeds meer met elkaar vervlochten.

Digitalisering brengt ook risico's met zich mee. Het leidt tot vraagstukken rondom het verzamelen van data en de verschillende vormen van classificatie daarbinnen. Denk daarbij in het bijzonder aan persoonsgegevens. Met welk doel worden ze verzameld, wie beslist hierover, wie heeft ervoor getekend? En indien je met de juiste doelbinding beschikt over data hoe ga je er dan qua beveiliging mee om, zodat je voorkomt dat ze in verkeerde handen kunnen vallen.

Kennisnet ondersteunt het onderwijs in de zorg voor informatiebeveiliging en privacy. Omdat we daarbij zelf het goede voorbeeld willen geven moet informatiebeveiliging en privacy voor de Kennisdiensten en organisatie natuurlijk ook op orde zijn. In dit document laten wij zien aan iedereen met wie wij samenwerken, intern en extern, hoe wij dat georganiseerd hebben.

Voor Kennisnet zijn Informatiebeveiliging en privacy onlosmakelijk met elkaar verbonden en integraal onderdeel van beleid, processen en uitvoering. We hebben gekozen voor ISO 27001 als verzameling van beveiligingsmaatregelen om ons continue proces van risicoafweging en mitigerende maatregelen vorm te geven. Verder geldt *het by design principe* binnen Kennisnet voor alle dienstverlening, zowel voor security als voor privacy. Dit zorgt er ook voor dat IBP geen papieren tijger is of wordt maar een onderdeel van onze dagelijkse werkwijze.

Marianne Mulder
Directeur Operations

Inhoud

1. Het belang van informatiebeveiliging en privacy

Informatie en ict zijn de kernactiviteiten van Kennisnet. Hierbij hebben we te maken met een groot aantal mogelijke bedreigingen. Alle systemen die we gebruiken en gegevens die we bewaren en verwerken, kunnen worden bedreigd door bijvoorbeeld een aanval, een vergissing of de natuur (zoals een overstroming of brand).

Datalekken, incorrecte gegevens of diensten die niet beschikbaar zijn - in het ergste geval schaden deze incidenten onze bedrijfsvoering en daarmee het vertrouwen in Kennisnet. Daarom zijn de continuïteit van onze dienstverlening en privacybescherming van groot belang. Ook treffen we gericht maatregelen om mogelijke risico's tot een aanvaardbaar niveau te reduceren.

De directie doet daarom een beroep op iedereen die betrokken is bij de activiteiten van Kennisnet, vanuit een gemeenschappelijke visie en wil, de verwerking van (persoons)gegevens correct te laten verlopen.

Dit beleid gaat dieper in op de bescherming van ict en in het bijzonder persoonsgegevens. Het dient als norm en leidraad voor alle informatieverwerking en biedt een uitgangspunt voor audit en controle.

Dit beleid biedt elke belanghebbende – medewerker, klant of leverancier – een inzage in de manier waarop we omgaan met persoonsgegevens.

1.1. De scope van het informatiebeveiligings- en privacybeleid

Het informatiebeveiligings- en privacybeleid is van toepassing op alle informatieverwerking binnen en namens Kennisnet. Het beleid is van toepassing op onze eigen medewerkers, tijdelijk personeel en op personeel dat door derden wordt ingezet om diensten te verlenen aan of namens onze organisatie.

1.2. Het doel van informatiebeveiliging en privacy

Het Informatiebeveiligings- en privacybeleid binnen Kennisnet heeft de volgende doelen:

- Het waarborgen van de continuïteit van de dienstverlening van Kennisnet.
- Het beschermen van de privacy van eenieder van wie Kennisnet persoonsgegevens verwerkt.
- Het voorkomen en zo goed mogelijk afhandelen van incidenten.
- Het minimaliseren van de eventuele gevolgen van incidenten.

Bij het realiseren van deze doelen bewaakt Kennisnet de balans tussen werkbaarheid – in de meest brede zin van het woord – en informatiebeveiliging en privacy.

2. Het beleid

Het beleid bestaat uit keuzes die Kennisnet maakt om de doelen rond informatiebeveiliging en privacy te bereiken.

2.1. Voorbeeldrol

Kennisnet heeft een voorbeeldrol in de onderwijsketen en communiceert helder en actief over informatiebeveiliging en privacy. Alle medewerkers en diensten van Kennisnet dienen voorbeeldig te zijn wat betreft informatiebeveiliging en privacy.

2.2. Wet- en regelgeving

Kennisnet houdt zich aan alle relevante wet- en regelgeving. Twee regels vormen daarbij de basis:

- De bestuurder van Kennisnet is eindverantwoordelijk voor de bescherming van persoonsgegevens.
- Kennisnet hanteert passende technische en organisatorische maatregelen voor het beschermen van diensten en in het bijzonder persoonsgegevens.

2.3. IBP is overal in verweven

Kennisnet beschouwt informatiebeveiliging en privacy als onlosmakelijk met elkaar verbonden en als belangrijk onderdeel van het beleid, de processen en de uitvoering van diensten. Daar waar mogelijk wordt informatiebeveiliging en privacy opgenomen in bestaande processen.

2.4. IBP is de verantwoordelijkheid van iedereen

Omdat iedereen binnen en rondom Kennisnet bijdraagt aan informatiebeveiliging en privacy, zijn de rollen en verantwoordelijkheden rondom informatiebeveiliging en privacy duidelijk vastgelegd.

2.5. ISO 27001 als basis

Kennisnet kiest ISO 27001 (en ISO 27002) als een verzameling van geschikte beveiligingsmaatregelen. Hierbij is het proces voor informatiebeveiliging doorlopend en cyclisch. Dat betekent dat Kennisnet jaarlijks de organisatie als geheel evalueert, controleert en verbetert. Nieuwe ontwikkelingen of incidenten, binnen en buiten Kennisnet, aanschaf van diensten of bedrijfsmiddelen en grote wijzigingen in de dienstverlening zijn aanleiding tot extra valuatie, controle en eventuele bijstelling.

Kennisnet past classificatie, privacy *by design*, security *by design* en privacy *by default* toe om passende maatregelen te kunnen treffen.

3. Uitvoering

Om het informatiebeveiligings- en privacybeleid te realiseren, besteedt Kennisnet aandacht aan een aantal zaken.

3.1. Bewustzijn

Het bevorderen van bewustzijn rondom informatiebeveiliging en privacy is de verantwoordelijkheid van alle medewerkers. Het beveiligingsbewustzijn wordt vergroot door:

- Voorlichting (security awareness training)
- Opstellen en uitdragen van gedragsregels (handleiding aanvaardbaar gebruik bedrijfsmiddelen)

Deze middelen dragen het volgende uit:

- Het belang van informatiebeveiliging en privacy voor Kennisnet
- Nieuwe ontwikkelingen op het gebied van informatiebeveiliging en privacy (bijvoorbeeld actuele incidenten)
- De belangrijkste veiligheidsmaatregelen rond dagelijkse werkzaamheden
- Waar mensen terecht kunnen bij incidenten of met ideeën en vragen

3.2. Incidenten en datalekken

Medewerkers die een incident of inbreuk rond informatiebeveiliging en/of privacy vermoeden, dienen dit te melden. Een vraag of suggestie over informatiebeveiliging en privacy kan ook als incident gemeld worden. Alle meldingen worden volgens een vast proces behandeld.

Een interne medewerker kan melding doen bij de Servicedesk of via email naar security@kennisnet.nl. Wanneer het om persoonsgegevens gaat, wordt de Functionaris voor de Gegevensbescherming (FG) ingeschakeld. Na afhandeling van het incident wordt de melder ingelicht over de afhandeling daarvan.

Een melding van incidenten of verzoeken rondom persoonsgegevens door externe partijen kan gedaan worden bij de Servicedesk, of via email naar support@kennisnet.nl. In de standaard gebruiksvoorwaarden en disclaimer van Kennisnetdiensten, staat deze loketfunctie vermeld. Externe partijen kunnen bij dit loket terecht voor:

- Algemene informatie over de verwerking van persoonsgegevens.
- Verzoeken voor inzage van de eigen verwerkte gegevens en eventuele wijziging of verwijdering daarvan.

3.3. Naleving

Schending van de wetgeving, voorschriften of regels rond informatiebeveiliging en privacy kan leiden tot corrigerende maatregelen zoals non-actiefstelling, disciplinaire straffen en beëindiging van een contract of dienstverband.

3.4. Actualiteit

Kennisnet houdt rekening met actuele ontwikkelingen. Daarom wordt dit beleid minimaal elke twee jaar getoetst en bijgesteld door het managementteam (MT) aan de hand van het volgende:

- De behoeften en verwachtingen van belanghebbenden in de onderwijsketen
- De status van de informatiebeveiliging als geheel (beleid, organisatie, risico's)
- De effectiviteit van de genomen maatregelen en aantoonbare werking daarvan
- Wet- en regelgeving

3.5. Wet- en regelgeving

Kennisnet voldoet aan alle wet- en regelgeving die relevant is in dit verband:

- De Algemene Verordening Gegevensbescherming
- Het Privacyconvenant
- Het Normenkader privacy onderwijs
- De Archiefwet – in het bijzonder bewaartermijnen

Daarnaast zijn ook onderwijsstandaarden van toepassing, zoals de ROSA-katern IBP.

3.6. De vijf vuistregels van privacy

Kennisnet houdt zich bij het verwerken van persoonsgegevens aan de beginselen rond de verwerking persoonsgegevens (art.5 AVG). De **vijf vuistregels** van privacy zijn:

1. **Doelbepaling en doelbinding**: persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld. Persoonsgegevens worden niet verder verwerkt voor andere doeleinden.
2. **Grondslag**: verwerking van persoonsgegevens is gebaseerd op een van de wettelijke grondslagen.
3. **Dataminimalisatie**: bij de verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt. Het type persoonsgegevens staat in verhouding tot het doel - het doel kan niet met minder of alternatieve gegevens worden bereikt. Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.

4. **Transparantie**: Kennisnet legt aan betrokkenen (zoals leerlingen, hun ouders en medewerkers) op transparante manier en ongevraagd verantwoording af over het gebruik van hun persoonsgegevens en het beleid daarover. Daarnaast hebben de betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens. Ook kunnen betrokkenen zich geheel verzetten tegen het gebruik van hun persoonsgegevens.
5. **Data-integriteit**: er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn.

3.7. Dataregister

Alle verwerkingen binnen en namens Kennisnet worden vastgelegd en up-to-date gehouden in een dataregister.

3.8. Planning & controle

Kennisnet doorloopt een jaarlijkse planning- en controlecyclus voor informatiebeveiliging en privacy, deze bestaat minimaal uit de volgende activiteiten:

- **Risico-inventarisatie en selectie van maatregelen**. In het eerste kwartaal van elk jaar vindt een risicoworkshop plaats om de grootste risico's te identificeren. De resultaten hiervan bepalen welke informatiebeveiligingsmaatregelen geïmplementeerd of verbeterd dienen te worden in dat jaar.
- **Controle en rapportage**
  - Operationele controle op de naleving van beleid en richtlijnen wordt verricht door het lijnmanagement. De CTO rapporteert elk kwartaal aan het MT over de informatiebeveiliging binnen Kennisnet, de vorderingen rond implementatie en verbetering van maatregelen en de incidenten in dat kwartaal. Aan het einde van het jaar rapporteert de CTO over de implementatie van informatiebeveiligingsmaatregelen die uit de risicoworkshop zijn gekomen.
  - Interne audit: controle op de implementatie en borging van het informatiebeveiligings- en privacybeleid en de richtlijnen en maatregelen die hieruit voortkomen. Deze vindt gedurende het jaar plaats en wordt gedetailleerd beschreven in het 'Handboek interne audit informatiebeveiliging en privacy'. Rapportage vindt plaats aan de CTO.
  - Externe audit: minimaal jaarlijks een onafhankelijke controle van de informatiebeveiliging van één of meerdere onderdelen van de primaire bedrijfsvoering van Kennisnet. Rapportage vindt plaats aan de Directeur Operations.

4. Organisatie

Kennisnet verdeelt de rollen en verantwoordelijkheden voor informatiebeveiliging en privacy als volgt:

4.1. Medewerkers

Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging in hun dagelijkse werkzaamheden, zoals beschreven in het Personeelshandboek en de 'Handleiding acceptabel gebruikmaken van bedrijfsmiddelen'. Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met checklists en formulieren.

Wij vragen medewerkers zich actief bezig te houden met informatiebeveiliging. Bijvoorbeeld door meldingen te maken van security incidenten, verbetervoorstellen te doen en invloed uit te oefenen op het beleid binnen Kennisnet (individueel of via de OR).

4.2. Management

De bestuurder is de eindverantwoordelijke voor informatiebeveiliging en privacy.

Het MT is verantwoordelijk voor:
- Het vaststellen van het informatiebeveiligingsbeleid en de daaruit volgende richtlijnen voor Kennisnet.
- Het evalueren van de toepassing en werking van het informatiebeveiligings-beleid op basis van rapportages.

Binnen het MT is de Directeur Operations portefeuillehouder voor informatiebeveiliging en privacy. De CTO is verantwoordelijk voor het organiseren van informatiebeveiliging en privacy binnen Kennisnet.

Het lijnmanagement:
- Ziet toe op de naleving van het informatiebeveiligings- en privacybeleid door medewerkers.
- Heeft een positieve en actieve houding ten aanzien van informatiebeveiliging en privacy.
- Fungeert als voorbeeldfunctie.
- Behandelt informatiebeveiliging in bijvoorbeeld werkoverleg en beoordelingen.
- Handelt vertrouwelijke informatiebeveiligingsincidenten af.

4.3. Specifieke verantwoordelijkheden

Voor de uitvoering van het informatiebeveiligings- en privacybeleid zijn onder meer nodig: beleidsvoorbereiding, beheer van de processen, richtlijnen en procedures en controle op de naleving daarvan. Kennisnet verdeelt deze verantwoordelijkheden als volgt:
- **De Domeinmanager Exploitatie** houdt de centrale geautomatiseerde informatievoorziening en de beveiliging daarvan in stand.
- **De Manager P&O** beheert het personeelsbeleid van Kennisnet. Dit raakt de informatiebeveiliging en privacy wat betreft de selectie, de voorlichting en het ontslag van personeel en het gebruik en delen van personeelsgegevens. het gebruik en delen van personeelsgegevens.
- **De Officemanager** is verantwoordelijk voor de huisvesting. Binnen informatiebeveiliging is vooral de fysieke beveiliging van het kantoorpand een belangrijk thema.
- **De Controller** is verantwoordelijk voor de informatiebeveiliging rond administratieve procedures.
- **De Functionaris voor de Gegevensbescherming (FG)** houdt toezicht op de naleving van de Wet bescherming persoonsgegevens binnen Kennisnet. Hij of zij doet aanbevelingen voor een betere bescherming van persoonsgegevens. De CTO en de FG zorgen voor een goede taakverdeling rond informatiebeveiliging en privacybescherming binnen Kennisnet. De FG meldt voorgenomen verwerking van persoonsgegevens, indien nodig, aan de toezichthouder.
- **Het Hoofd BHV** is, wat informatiebeveiliging en privacy betreft, verantwoordelijk voor het duiden van veiligheidsvoorzieningen rond de fysieke veiligheid van Kennisnetmedewerkers.
- **De Security Officer** is het technische aanspreekpunt rond informatiebeveiliging binnen Kennisnet.
- **De Servicedeskmedewerkers** beheren het loket voor inzageverzoeken en meldingen