Beleid in kader van de Wet Meldplicht Datalekken

Inhoud:

1. Achtergrond

Eind jaren 80 van de vorige eeuw werd de wet- en regelgeving rondom beveiliging persoonsgegevens voor het eerst ingevoerd. Het begon met de Wet Persoonsregistratie (WPR) in 1989. Deze wet stelde regels aan het gebruik van persoonsgegevens die door een bedrijf of instelling voor een bepaald doel werden verzameld. In de daaropvolgende jaren breidde de overheid de wet en regelgeving meer en meer uit. Zorggroep Ena heeft haar Privacy Reglement hierop gebaseerd. Het beleid volgend uit de Wet Melding Datalekken is aanvullend op het Privacy Reglement.
Per 1 januari 2016 is aan de WBP de "Wet Meldplicht Datalekken" toegevoegd. Deze meldplicht houdt in dat organisaties (zowel bedrijven als overheden) direct een melding moeten doen bij de Autoriteit Persoonsgegevens (het voormalige College Persoonsbescherming) zodra zij een ernstig datalek hebben. Soms is het ook verplicht het datalek te melden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt). De verplichtingen die voorheen werden gesteld in de Wet Bescherming Persoonsgegevens (WBP) privacy gebied en de uitvoering hiervan, worden met de meldplicht nu nog strenger gehandhaafd.
Het gebruik van datacommunicatiemogelijkheden (internet, E-commerce) neemt steeds meer toe. De complexiteit van en verwevenheid tussen geautomatiseerde systemen, de massaliteit van de dagelijkse communicatie, de omvang van de bestanden alsmede de toenemende professionalisering van de computercriminaliteit leiden tot een grote afhankelijkheid en kwetsbaarheid van de geautomatiseerde informatievoorziening binnen Zorggroep Ena. De risico's die hiermee samenhangen zijn zeer aanzienlijk en kunnen een bedreiging vormen voor de vertrouwelijkheid, integriteit en continuïteit van de geautomatiseerde informatievoorziening en daarmee indirect voor het imago en dus de continuïteit van Zorggroep Ena.
In het kader van de Wet Meldplicht Datalekken zijn de beleidsuitgangspunten betreffende bescherming persoonsgegevens zoals beschreven in het Privacy Reglement van Zorggroep Ena, aangescherpt. Het beleidsdocument maakt deel uit van het complete privacy- en beveiligingsbeleid van Zorggroep Ena.

2. Verantwoordelijkheid Zorggroep Ena

Gelet op de mogelijke impact van verstoringen op de continuïteit van Zorggroep Ena berust eindverantwoordelijkheid voor het beleid betreffende de beveiliging en de interne controle van de geautomatiseerde informatievoorziening bij de Raad van Bestuur.

3. Doelstelling en doelgroep

De beleidsdoelstelling betreffende de vertrouwelijkheid, integriteit en continuïteit van de geautomatiseerde informatievoorziening van de Zorggroep Ena luidt:
"Het bieden van een raamwerk van beleidsuitgangspunten met betrekking tot de exclusiviteit, integriteit en beschikbaarheid van de geautomatiseerde informatievoorziening, waarbinnen een evenwichtig (doeltreffend en doelmatig) stelsel van onderling samenhangende maatregelen ontwikkeld wordt, teneinde de geautomatiseerde informatievoorziening te beschermen tegen interne en externe bedreigingen."
Alle leidinggevenden dienen ervoor zorg te dragen, dat aan de in dit protocol geformuleerde beleidsuitgangspunten wordt voldaan bij de inrichting van de organisatie, procedures, werkwijze en de daarbij gehanteerde informatiesystemen.

4. Partijen met verschillende rollen en taken

- Zorggroep Ena is houder en daarmee eindverantwoordelijke voor de door haar gebruikte geautomatiseerde informatiesystemen. ICT is ondergebracht bij de Economische en Administratieve Dienst die Itannex aanstuurt.
- Systeembeheerder, gedetacheerd naar Itannex, is verantwoordelijk voor de infrastructuur (werkstations, Servers, netwerk) en fysieke beveiliging en controle maatregelen
- De systeemontwikkelingsorganisatie (leverancier applicaties) is verantwoordelijk voor het realiseren van de overeen te komen gewenste functionele specificaties tijdens systeemontwikkelingstrajecten.
- Applicatiebeheerder is verantwoordelijk voor de gebruikersondersteuning op uitvoerend niveau binnen de organisatie en is intermediair tussen de Zorggroep en de systeemontwikkelingsorganisaties.
- Bewerker is degene die de gegevens namens Zorggroep Ena verwerkt en bewerkt
- Betrokkenen zijn degene over wie de persoonsgegevens gaan. Dit kunnen cliënten of werknemers van Zorggroep Ena zijn. De betrokkene heeft een aantal rechten namelijk:
    - Recht op informatie: welke gegevens worden verwerkt en waarom
    - Recht om vragen te stellen: welke gegevens zijn in bezit van de organisatie
    - Recht van toegang: betrokkene mag altijd kennis hebben van zijn gegevens
    - Recht van verzet: indien de betrokkene ernstige bezwaren heeft tegen het gebruik van de gegevens, mag deze zich daartegen verzetten. Dat kan niet als het gaat om gegevensverwerking die is opgelegd door een wet of reglementaire bepaling of die noodzakelijk is voor de uitvoering van de overeenkomst met de organisatie.
    - Recht op spoedige afhandeling van verzoeken op basis van genoemde rechten binnen 4 weken.

5. Informatiebeveiliging

De eindverantwoordelijkheid ligt bij Zorggroep Ena, ook als een aantal aspecten van het informatiesysteem uitbesteed wordt aan derden. Dit kan zowel betrekking hebben op aspecten tijdens de ontwikkeling van het systeem, als tijdens het beheer, het gebruik en/of bepaalde deelcomponenten van het totale systeem.
De te treffen maatregelen ter bescherming van privacy gevoelige gegevens, evenals de prioriteitsstelling hierin, dienen te worden bepaald op grond van een door het bedrijfsonderdeel periodiek op te stellen risicoanalyse, waarin de bedreigingen tegen een betrouwbare en op continuïteit gerichte, geautomatiseerde informatievoorziening en de daarmee samenhangende risico's worden onderkend en een evenwichtig stelsel van onderling samenhangende maatregelen wordt ontwikkeld ter reducering van de risico's tegen acceptabele kosten.
Hierbij wordt daarom niet een maximaal beveiligingsniveau nagestreefd, maar een optimaal niveau. Bij het uitvoeren van de jaarlijkse risicoanalyse wordt Zorggroep Ena ondersteund door Itannex.
Itannex vervult in deze een coördinerende rol, opdat overlappingen en tekortkomingen in het totale stelsel van maatregelen binnen de Zorggroep Ena worden voorkomen.

6. Beleidsuitgangspunten

De WBP kent een aantal uitgangspunten die als voorwaarden gelden bij het verwerken van persoonsgegevens:

- Doelbinding: Het is alleen toegestaan persoonsgegevens te verwerken om het vooraf vastgestelde doel te bereiken. Gegevens die daarmee niet in verband staan, mogen dus niet verzameld worden. Ook de juiste beveiligingsmaatregelen dragen eraan bij dat de gegevens niet voor een verkeerd doel worden gebruikt.
- Grondslag: Persoonsgegevens mogen alleen verwerkt worden als de WBP hier een grond voor noemt. Een aantal voorbeelden hiervan zijn:
    - Toestemming: de betrokkene geeft toestemming
    - Overeenkomst: de gegevensverwerking is noodzakelijk voor de uitvoering van de overeenkomst met de betrokkene.
    - Wet: de wetgeving eist dat persoonsgegevens verwerkt worden.
- Dataminimalisatie: De persoonsgegevens die als organisatie verwerkt worden verwerkt, dienen redelijkerwijs nodig te zijn om het doel te bereiken. De gegevens staan in verhouding tot het doel ('proportioneel'). Zonder de verzamelde gegevens is het niet mogelijk het doel te bereiken ('subsidiair'). Alleen gegevens die écht nodig zijn om het doel te bereiken, worden verzameld.
- Transparantie en rechten van de betrokkene: De betrokkene is vooraf in begrijpelijke taal geïnformeerd over wat er precies aan informatie wordt verwerkt en wat het doel daarvan is. In het geval van een wilsonbekwame betrokkene, is ook de wettelijke vertegenwoordiger op de hoogte van hun rechten als het gaat om de verwerking van persoonsgegevens.

Vanuit Zorggroep Ena worden deze uitgangspunten aangevuld met:

- De fysieke en logistieke beveiliging van de computerruimten en op de locaties van Zorggroep Ena is zodanig, dat de vertrouwelijkheid, integriteit en beschikbaarheid van de gegevens en gegevensverwerking gewaarborgd zijn.
- Aanschaf, installatie en onderhoud van geautomatiseerde gegevensverwerkende systemen, evenals inpassing van nieuwe technologieën, mogen geen afbreuk doen aan het niveau van veiligheid van de totale informatievoorziening
- Het personeelsbeleid is mede gericht op het leveren van een bijdrage aan de integriteit, vertrouwelijkheid en continuïteit van de informatievoorziening.
- Opdrachten aan derden voor het uitvoeren van werkzaamheden worden zodanig omgeven met maatregelen, dat er geen inbreuk op de vertrouwelijkheid, integriteit en continuïteit van de informatievoorziening kan ontstaan.
- Bij de verwerking en het gebruik van gegevens worden maatregelen getroffen om de privacy van klanten en personeel te waarborgen.
- Logische toegangsbeveiliging zorgt ervoor, dat ongeautoriseerde personen of processen geen toegang krijgen tot de geautomatiseerde systemen, gegevensbestanden en programmatuur van Zorggroep Ena
- Gegevensverstrekking intern en extern gebeurt op basis van 'need to know'. Medewerkers treffen maatregelen om te voorkomen dat informatie in handen van personen terechtkomt, die deze informatie niet strikt nodig hebben. Ook de toegang tot informatiesystemen wordt volgens dit principe adequaat beveiligd. Voor ICT-beheerders en applicatiebeheerders wordt hierop een uitzondering gemaakt, om te komen tot een betere service aan de bewerkers.
- Datatransport is zodanig met beveiligingsmaatregelen omkleed, dat geen inbreuk kan worden gepleegd op de vertrouwelijkheid en de integriteit van de gegevens en op de informatievoorziening als geheel.

- Om computervirusinfecties te voorkomen wordt er slechts gewerkt met geautoriseerde versies van (legale) programmatuur.
- Het beheer en de opslag van gegevens (back-up) zijn zodanig, dat geen informatie verloren kan gaan.
- Er zijn calamiteitenplannen en -voorzieningen om de continuïteit van de bedrijfsvoering en de informatievoorziening te waarborgen en imagoschade te voorkomen en lessen te trekken uit deze calamiteiten.

7. Risico op datalekken

Een datalek wil zeggen dat persoonsgegevens zijn blootgesteld aan verlies of aan onrechtmatig gebruik. Voorbeelden hiervan zijn: gestolen apparatuur, een verloren USB stick, inbraak door een hacker, malware (oftewel een virus) of een brand. Wanneer er alleen sprake is van een zwakke plek in de beveiliging, is dat geen datalek, maar een beveiligingslek.

Zorggroep Ena is niet verplicht elk datalek te melden. In de beleidsregels is aangegeven dat 'ernstige'
datalekken zonder onnodige vertraging en zo mogelijk niet langer dan 72 uur na ontdekking van het datalek bij de toezichthouder moeten worden gemeld. Een lek is ernstig als het een grote hoeveelheid data betreft (kwantitatief ernstig), maar ook wanneer het om gevoelige gegevens gaat (kwalitatief ernstig). Een paar voorbeelden van gevoelige gegevens zijn:
• Inloggegevens
• Financiële gegevens
• Kopieën van identiteitsbewijzen
• Werkprestaties
• Gegevens die betrekking hebben op levensovertuiging
• Gegevens die betrekking hebben op gezondheid

De meest in het oog springende applicaties waar persoonsgegevens zijn opgeslagen zijn
- CURA (HRM gegevens)
- ECD (Elektronisch Cliëntendossier met cliëntgegevens en zorgplannen)
- OMAHA
- SDB salarisverwerking
- VECOZO (dataverkeer cliëntgegevens)

Door systeembeheerder Itannex zijn in overleg met Zorggroep Ena maatregelen getroffen ter beveiliging van de data en ter voorkoming van misbruik van gegevens. In de bijlage zijn deze maatregelen opgenomen.

Het gebruik van Social media zoals facebook, Istagram, LinkedIn, etc. neemt steeds meer toe.
Deze media worden voor allerlei doeleinden gebruikt om met elkaar zaken en gebeurtenissen te delen. Dit kan persoonlijk zijn maar ook werk gerelateerd.
Echter, ook hier geldt dat persoonsgegevens in de vorm van namen maar ook foto's van bewoners, bezoekers of medewerkers zonder toestemming van betrokkenen niet gedeeld mogen worden.
Het gebruik van social media heeft naast de positieve mogelijkheden ook het risico in zich dat de privacy van mensen geschonden wordt.

8. Calamiteitenplan bij datalekken:

In het kader van het Wet Bescherming Persoonsgegevens, aangevuld met de Wet Meldplicht Datalekken dient een calamiteitenplan opgesteld te worden voor het geval er sprake is van het lekken van privacy gevoelige data.
Bij constatering van datalekken worden de volgende stappen volgens de volgende stappen ondernomen:

1. Ontdekking

Het datalek wordt ontdekt door eigen waarneming, na een klacht of melding uit een systeem en gemeld bij de applicatiebeheerder of de systeembeheerder Itannex:
De applicatie wordt door hen direct gesloten om verdere datalekkage te voorkomen.

2. Inventarisatie

De applicatiebeheerder, systeembeheerder Itannex en het hoofd EAD vormen een ad hoc werkgroep die een analyse maakt van het datalek. De Raad van Bestuur wordt door de werkgroep op de hoogte gesteld van het datalek en de daaruit volgende stappen.

Omschrijving datalek:

- wat is er gebeurd? Details!
- Wat is de oorzaak?
- Wanneer plaatsgevonden?
- Welke (typen) persoonsgegevens?
- Hoe veel betrokkenen?
- Soort betrokkenen
- Zijn er contactgegevens van de betrokkenen? Wie zijn de betrokkenen? (identificatie!)
- Eigen contactgegevens ontdekker

Daarnaast wordt geïnventariseerd:

- Wat zijn de privacy gevolgen voor de betrokkene?
- Wordt/worden de betrokkene(n) geïnformeerd?
- Inhoud melding bepalen op basis van de inventarisatie
- Welke technische en organisatorische maatregelen om datalek te verhelpen/voorkomen?
- Inschatting maken van (on-)begrijpelijkheid gegevens voor onbevoegden.

3. Beoordeling

De werkgroep beoordeelt of het datalek meldingswaardig is t.a.v. de Autoriteit Persoonsgegevens (=Toezichthouder) en betrokkenen. De werkgroep hanteert daarvoor de volgende checklist:

- Gevoelige persoonsgegevens (bijvoorbeeld medisch, religie, financieel, etc.)
- Andere factoren zoals gevoelige verwerkingen (vb. Gegevens onder geheimhouding, kwetsbare groep betrokkenen, veel betrokkenen)
- Niet de betrokkenen informeren als de gelekte informatie onbegrijpelijk gemaakt is voor onbevoegden (goede encryptie)

4. Reparatie

Na achterhalen oorzaak datalek wordt de reparatie met voorrang uitgevoerd door applicatiebeheer-der en/of systeembeheerder Itannex

5. Melding

De Raad van Bestuur stelt de Autoriteit Persoonsgegevens onverwijld in kennis van een inbreuk op de beveiliging, bedoeld in artikel 13 die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens.
De Raad van Bestuur meldt:

- Zodra alle benodigde informatie beschikbaar is
- Onverwijld (dit is binnen 48 uur) is niet altijd haalbaar
- Tijdige principemelding/ pro formamelding gevolgd door vervolgmelding of intrekking
- Verlate complete melding met als risico dat de Autoriteit Persoonsgegevens dit niet accepteert binnen Wet Meldingsplicht Persoonsgegevens.

De Raad van Bestuur stelt de betrokkene(n) onverwijld in kennis van de inbreuk op de beveiliging van persoonsgegevens, indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer. Dit op basis van de bevindingen van stap 3 van het calamiteitenplan.

6. Documentatie

De werkgroep verzorgt t.b.v. de Raad van Bestuur voor goede verslaglegging van de casuïstiek:

- Alle informatie uit voorafgaande stappen
- Alle informatie van melding zelf
- Afschrift melding bij toezichthouder en kopie melding aan betrokkenen.

9. Gegevens Toezichthouder Autoriteit Persoonsgegevens:

Melding wordt gedaan met gebruik van het meldingsformulier op de site van de Autoriteit Persoonsgegevens:

www.autoriteitpersoonsgegevens.nl

10. Bijlage: Netwerk beveiliging Zorggroep Ena

Het netwerk van Zorggroep Ena is op de volgende punten beveiligd:

- *Wachtwoordbeleid:*
  Voor de meeste gebruikers moet het wachtwoord elk half jaar gewijzigd worden.
  Het wachtwoord moet minimaal 6 tekens bevatten.
  Uitzonderingen zijn afdeling gebruikers, die een algemeen account gebruiken, zoals keukens, afdelingen enz.

- *Toegang netwerk:*
  Voor de toegang tot het netwerk is een geldig gebruikersaccount vereist.
  Bij 30 minuten inactiviteit moeten de gebruikers gegevens opnieuw worden ingevoerd (Schermbeveiliging).
  Er is voor een beperkt aantal medewerkers een VPN verbinding beschikbaar gesteld om vanaf huis in te kunnen loggen.

- *Virusbescherming*
  Alle servers en werkplekken zijn beschermd met een Virusscanner die regelmatig wordt bijgewerkt.
  Op de mailserver draait een SPAM filter, die het grootste deel van de ongewenste e-mail blokkeert.

- *Opslag van gegevens*
  Wij maken gebruik van centrale opslag van gegevens, dat wil zeggen dat alle gegevens worden bewaard op een centrale dataserver. Gegevens worden niet of nauwelijks lokaal opgeslagen. Mede dankzij gebruik van Server Based Computing wordt dit zoveel mogelijk voorkomen.

- *Beveiliging per applicatie*
  Ter bescherming van privacygevoelige informatie ontwikkelen producenten aanvullende beveiligingsprocedures. Concrete voorbeelden zijn VeCoZo en Unit4. Voor Unit4 geldt voor de applicatie 'Verzuimsignaal' dat vanaf voorjaar 2016 het inloggen door middel van authenticatie in twee stappen. Voor medische gebruikers is dit een verplichting in het vanaf 2016.