leeuwenborgh
vakmensen in opleiding

Hoe kunt u helpen bij informatiebeveiliging en privacy?

Auteur : S. Rodolf-Lejeune
Versie : 0.9
Datum : 24-5-2018
Status : Concept

leeuwenborgh
vakmensen in opleiding

Inleiding:

Informatiebeveiliging en privacy zijn belangrijke punten in een organisatie zoals Leeuwenborgh. Met 800 medewerkers en ruim 8500 studenten worden veel persoonsgegevens verwerkt. Er zijn reeds documenten opgesteld inzake het informatiebeveiligings- en privacybeleid maar met de komst van de Algemene Verordening Gegevensbescherming, die vanaf 25 mei 2018 geldt in Nederland, is het noodzaak om de procedures en de gevaren inzake de informatiebeveiliging en privacy, nogmaals toe te lichten.

Dit betekent niet dat privacy een hype is. Privacy bestaat al jaren maar door de ontwikkeling van het internet en de sociale media wordt het bewustzijn minder en wordt de kans op inbreuk groter.

leeuwenborgh
vakmensen in opleiding

Inhoud

leeuwenborgh
vakmensen in opleiding

1. Uitgangspunten en –principes informatiebeveiliging

1.1 Uitgangspunten

Informatiebeveiliging en privacy is een lijnverantwoordelijkheid maar tevens de verantwoordelijkheid van iedere medewerker en dientengevolge zal iedereen zich in gedrag en houding hiernaar moeten richten.
Veilig en betrouwbaar omgaan met informatie in het dagelijks werk is ieders professionele verantwoordelijkheid. Alle medewerkers dienen actief bij te dragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie. [1]

1.2 Wat is privacy?

"Het recht om met rust gelaten te worden en het recht gegevens over jezelf te kunnen controleren". Je moet erop kunnen vertrouwen dat jouw privacy wordt gerespecteerd.

2. Wat zijn persoonsgegevens?

Een persoonsgegeven is elk gegeven over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Er zijn twee soorten persoonsgegevens. Algemene persoonsgegevens kunnen onderverdeeld worden in direct of indirecte identificerend persoonsgegevens, zoals de naam en het adres. De bijzondere persoonsgegevens zijn de gegevens over onder andere gezondheid, ras en geaardheid.[2]

3. Verantwoordelijkheid medewerker

In hoofdstuk één en twee wordt het onderwerp privacy en persoonsgegevens toegelicht. Het geeft aan wat we wel en niet verkiezen te delen. De volgende hoofdstukken gaan over de werkwijze van het zorgen dat informatie die we privé willen houden, privé blijft.
De medewerker is daardoor verantwoordelijk voor:

- het naleven van het Informatiebeveiliging- en Privacybeleid, maatregelen en procedures;
- het meewerken aan Informatiebeveiligings- en Privacy controles en audits;
- het signaleren en melden van (mogelijke) Informatiebeveiliging- en Privacy incidenten en zwakke plekken;
- het (doen) bevorderen van het Informatiebeveiligings- en Privacy bewustzijn binnen Leeuwenborgh;
- deelname aan cursussen i.h.k.v. IBP-bewustwording. [3]

[1] Informatiebeveiligings- en privacy beleid ROC Leeuwenborg, N. Hermans e.a., Maastricht 2017, p.9.
[2] https://autoriteitpersoonsgegevens.nl/nl/over-privacy/persoonsgegevens/wat-zijn-persoonsgegevens.
[3] Informatiebeveiligings- en privacy beleid ROC Leeuwenborg, N. Hermans e.a., Maastricht 2017, p.23.

4. De 5 Vuistregels

Er zijn 5 vuistregels die de medewerker die persoonsgegevens verwerkt, dient na te komen om de informatiebeveiliging en privacy van de betrokkenen te *bevorderen*:

1. Doelbepaling en doelbinding: hier dient men rekening te houden met een vooraf vastgesteld en concreet doel. Deze persoonsgegevens mogen alleen worden verwerkt om dat vastgestelde doel te bereiken (doelbinding).
2. Grondslag: De grondslag is de verwerking van persoonsgegevens gebaseerd op een van de volgende wettelijke grondslagen: toestemming, overeenkomst, de wet, publiekrechtelijke taak, vitaal belang van de betrokkene, of gerechtvaardigd belang.
3. Dataminimalisatie: Bij dataminimalisatie dienen de persoonsgegevens die verwerkt worden, redelijkerwijs nodig te zijn om het doel te bereiken. De gegevens moeten in verhouding staan tot het doel ('proportioneel') en het doel kan niet met minder dan deze verzamelde gegevens worden bereikt ('subsidiair'). Het gaat er dus om dat uitsluitend gegevens verzameld worden die écht nodig zijn om het doel te bereiken. Niet: zo min mogelijk gegevens, wel: alleen relevante gegevens. Dataminimalisatie heeft ook te maken met bewaartermijnen en nog meer met het vernietigen van data als de bewaartermijn is verstreken.
4. Transparantie (rechten betrokkenen): Bij transparantie dient de betrokkene (dus: de student en/of zijn ouders) vooraf in begrijpelijke taal geïnformeerd te worden over wat er precies aan informatie wordt verwerkt en wat het doel daarvan is. De student en zijn ouders zijn op de hoogte van hun rechten als het gaat om de verwerking van persoonsgegevens door de school.
5. Data-integriteit: Bij data-integriteit zorgt de school er voor dat bij verwerkingen, die door of namens de school of schoolbestuur worden uitgevoerd, de juiste persoonsgegevens op het juiste moment op de juiste plaats beschikbaar zijn. Onjuiste gegevens worden op tijd gerectificeerd of gewist.

5. Praktijksituaties inzake het niet bewust omgaan met informatiebeveiliging en informatie.

5.1 Informatiebeveiliging

De privacy kan gewaarborgd worden als de informatiebeveiliging goed is geregeld. Ook bij informatiebeveiliging spelen de medewerkers een grote rol. De systemen kunnen goed beveiligd zijn maar als een vreemde bij deze informatie kan komen door het niet locken van de laptop bij het verlaten van de werkplek, kunnen de gegevens toch ongewild gedeeld worden. Daarom worden in de volgende alinea tips gegeven die een inbreuk kunnen voorkomen.

5.2 Tips naar aanleiding van praktijkvoorbeelden

De systemen zijn zodanig ingericht dat inbreuk op belangrijke informatie en privacy voorkomen kan worden. Voorkoming van verspreiding van informatie en beveiliging is ook een taak van de medewerkers. De volgende handelingen dienen naar aanleiding van praktijkvoorbeelden te worden gevolgd:

- Sla persoonsgegevens nooit onveilig op, zoals op een usb-stick of op je eigen, onbeveiligde harde schijf.
- Veeg het bord uit of verwijder beschreven papieren van de flipover.
- "Lock" altijd je laptop als je je werkplek verlaat.
- Ga zorgvuldig om met inloggegevens. Laat deze niet op een briefje rondslingeren en plak die zeker niet op je monitor.
- Klik nooit op een onbekende link in een mail van een onbekende afzender. Voor je het weet haal je malware binnen waardoor bestanden op je computer 'gegijzeld' worden.
- Wissel persoonsgegevens over studenten en medewerkers niet zomaar uit per e-mail, maar doe dat veilig via een systeem met wachtwoorden. Is de ontvanger de betrokkene, bijvoorbeeld een student die zijn of haar cijfer via de e-mail vraagt, zorg er dan voor dat alleen de persoonsgegevens met cijfer van deze persoon worden gestuurd.
- Deel wachtwoorden van studenten en medewerkers niet publiek op bijvoorbeeld het digibord.
- Log niet in als het digibord aanstaat, studenten kunnen dan meekijken.[4]

6. Beveiligingsincident.

Wordt niet voldaan aan voorgaande punten of is sprake van een diefstal of verlies van een laptop, telefoon of harde schijf, dan kan sprake zijn van een beveiligingsincident.

Als er een beveiligingsincident optreedt, is het van belang dit zo snel mogelijk te melden, zodat gewerkt kan worden aan een oplossing. Anderzijds is snel melden van belang zodat voor het beveiligingsincident kan worden beoordeeld of het wellicht een datalek betreft. Een beveiligingsincident zal altijd vertrouwelijk worden behandeld. Dit is van belang om de impact ervan niet onnodig te verhogen, hoe minder mensen weet hebben van een beveiligingsincident, hoe minder personen misbruik kunnen maken. Daarnaast is het van belang dat de vertrouwelijkheid van bedrijfsgegevens en wellicht de privacy van personen geborgd blijft.

Als er persoonsgegevens betrokken zijn bij het beveiligingsincident, bestaat de mogelijk dat het een datalek betreft. Naast het oplossen van het datalek en het treffen van maatregelen om herhaling in de toekomst te voorkomen, is Leeuwenborgh wellicht verplicht om het datalek te melden bij de Autoriteit Persoonsgegevens (AP). Als een datalek onterecht niet (op tijd) wordt gemeld, loopt Leeuwenborgh het risico op een fikse boete.

[4] https://www.kennisnet.nl/artikel/informatiebeveiliging-en-privacy-in-het-mbo-hoe-alert-ben-jij/.

7. Signalering en melden van (mogelijke) Informatiebeveiligings- en Privacy incidenten en zwakke plekken

7.1 Begrippen en toelichting

Wat is een beveiligingsincident
Een beveiligingsincident is een gebeurtenis die inbreuk maakt op bestaande (beveiligings)maatregelen. Door een beveiligingsincident kan de beschikbaarheid of de vertrouwelijkheid van informatie geschaad worden.

Wat is een datalek
Een datalek is een beveiligingsincident waarbij persoonsgegevens verloren zijn geraakt of onbevoegde toegang heeft plaatsgevonden.

Voorbeelden van beveiligingsincidenten en datalekken
Om een indruk te krijgen van beveiligingsincidenten en datalekken volgen nu enkele voorbeelden.

Beveiligingsincidenten:

- De website van Leeuwenborgh wordt gehackt.
- Computers van Leeuwenborgh worden gekaapt door een infectie met Ransomeware.
- Via het openen van spam worden virussen in het netwerk van Leeuwenborgh geïntroduceerd.
- Een PC of Laptop van Leeuwenborgh wordt gestolen.
- Een bezoeker heeft onbevoegd toegang tot een niet vergrendelde PC (werkplek) van Leeuwenborgh.

Datalekken (bijzonder soort beveiligingsincident):

- Een brief met persoonsgegevens wordt naar een verkeerd adres gestuurd en komt geopend retour.
- Op een gehackte PC staan persoonsgegevens opgeslagen.
- Een USB stick, harddisk, CD of DVD, met daarop persoonsgegevens, raakt kwijt.
- Papieren documenten met persoonsgegevens komen in handen van onbevoegde personen.

Persoonsgegevens
Persoonsgegevens zijn gegevens over een geïdentificeerde of identificeerbare natuurlijke persoon. Persoonsgegevens gaan direct over iemand of zijn te herleiden naar deze persoon. Dat het om een natuurlijk persoon moet gaan, houdt in dat gegevens van overleden personen geen persoonsgegevens zijn.

Voorbeelden van persoonsgegevens:

Soort persoonsgegevens	**Groep**	**Voorbeelden**
Directe	NAW	Naam, adres, telefoonnummer, email-adres,…
	Identificeerbare	Vingerafdruk, irisscan, foto, ……
Indirecte	Persoonskenmerken	Relatie, maatschappelijke status, geboortedatum, beroep, ……
	Lichamelijke kenmerken	Geslacht, lengte, gewicht, IQ, ….
	Behandelgegevens	Afspraken, opname, ziekenhuisnaam, arts, dieet, ….
	Financiën	Salaris, belasting, onkosten, vergoeding, schuldsanering, economische situatie, kredietinformatie, ….

Soort persoonsgegevens	Groep	Voorbeelden
Bijzondere	Gezondheid	Aandoening, medicijngebruik, samples (weefsel, DNA)
	Geloof en afkomst	Ras Godsdienst of levensovertuiging Seksuele leven (geaardheid)
	Overige	BSN Lidmaatschap van een vakbond Strafrechtelijk verleden Politieke voorkeur

Bij de volgende gebeurtenissen kan sprake zijn van een Privacy incident.

- De toestemming van betrokkene ontbreekt.
- Het juiste doel van de verwerking van de gegevens van de ontbreekt.
- Belangrijke gegevens van medewerkers en/ of studenten die in een gezamenlijk document naar meerdere mensen worden gestuurd maar waarvan de meeste informatie niet nodig is om in een bestand te verwerken. Zie BSN bij de rest van de gegevens. Naam adres enz.

7.2 Wat te doen bij een beveiligingsincident

Bij het optreden van een beveiligingsincident is van belang om dit snel (onverwijld) te melden via Topdesk. Voorzie de melding hierbij van voldoende informatie over het incident, zodat het oplossen eenvoudiger verloopt.

Het beveiligingsincident zal worden behandeld door het incidententeam en zal zorgvuldig geregistreerd worden. De afhandeling van het beveiligingsincident zal vertrouwelijk plaatsvinden volgens een standaardprocedure.

8. Gevolgen datalek

8.1 Datalek

Indien sprake is van een Informatiebeveiligings- en Privacy incident kan sprake zijn van een datalek . Een datalek kan(grote) gevolgen hebben voor Leeuwenborgh:
Mensenrechten worden geschonden, de zorgplicht van Leeuwenborgh wordt niet nagekomen, de accountscontrole kan niet positief worden beoordeeld, het imago van Leeuwenborgh kan enorm verslechteren en ten slotte kunnen hoge boetes opgelegd worden.

8.2 Contactgegevens binnen Leeuwenborgh inzake IBP

Bij vragen inzake de informatiebeveiliging en privacy kunt u terecht bij onze consulent informatiebeveiliging en privacy.
IBP@leeuwenborgh.nl

Bij een vermoeden van een datalek maakt u een melding in Topdesk onder het tabblad personeelservice of via de website via de knop ga direct naar AVG.