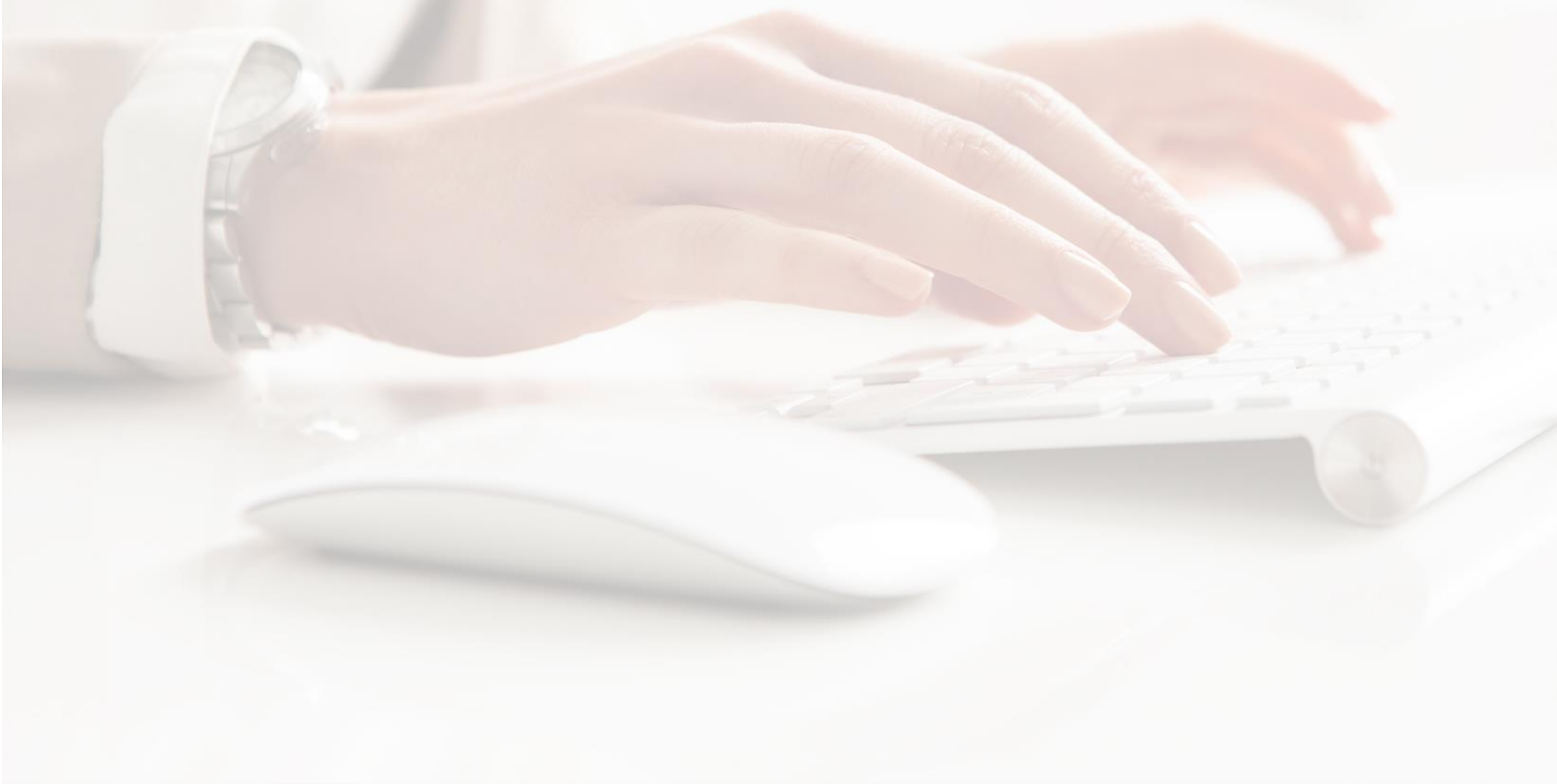
NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Datalekken en de rol van de IT-auditor

Factsheet

Versie 1.0 – december 2015



Datalekken

Sinds 1 januari 2016 is een wijziging van de Wet bescherming persoonsgegevens (Wbp) van kracht die een meldplicht regelt voor datalekken. Deze meldplicht houdt in dat bedrijven, overheden en andere organisaties die persoonsgegevens verwerken datalekken moeten melden aan de Autoriteit Persoonsgegevens (voorheen het College Bescherming Persoonsgegevens), en in bepaalde gevallen ook aan de betrokkene. De betrokkene is diegene van wie persoonsgegevens zijn gelekt. Het gaat hierbij om datalekken waarbij er kans is op verlies of onrechtmatige verwerking van persoonsgegevens.

De Autoriteit Persoonsgegevens heeft beleidsregels voor de meldplicht datalekken opgesteld. De bedrijven, overheden en andere organisaties tot wie de meldplicht datalekken zich richt, moeten zelf een beredeneerde afweging maken of een concreet datalek dat hen ter kennis komt onder het bereik van de wettelijke meldplicht valt. Doel van deze beleidsregels is om hen daarbij te ondersteunen. Deze beleidsregels dienen tevens als uitgangspunt voor het handhavingsbeleid van de Autoriteit Persoonsgegevens.

Rol van de IT-auditor

IT-auditing is het vakgebied dat zich bezighoudt met de beoordeling van en/of advisering over kwaliteitsaspecten van informatietechnologie. IT-auditors die voldoen aan de opleidings- en ervaringseisen zijn ingeschreven in het NOREA-register als gekwalificeerde IT-auditors (RE's).

De IT-auditor kan een uitstekende rol vervullen bij de gevolgen van de meldplicht datalekken, o.a. door:

1. Het inventariseren van verwerkingen van persoonsgegevens;
2. Het beoordelen van de gevoeligheid van de aanwezige gegevens;
3. Het uitvoeren of beoordelen van risicoanalyses;
4. Het beoordelen van de opzet, bestaan en werking van het stelsel van getroffen maatregelen gericht op de bescherming van persoonsgegeven;
5. Het beoordelen van de aanwezigheid van datalekken;
6. Het opstellen of beoordelen van procedures voor het ontdekken, beoordelen en opvolgen van eventuele datalekken;
7. Het adviseren over en beoordelen van verbetermaatregelen na geconstateerde datalekken.

De IT-auditor beschikt over kennis en ervaring om het risico dat de meldplicht datalekken met zich meebrengt voor bedrijven, overheden en andere organisaties te verminderen naar een beheersbaar niveau.

Aandachtspunten voor de IT-auditor

- De meldplicht datalekken of -in bredere zin - de Wet bescherming persoonsgegevens is principe gebaseerd. Dit betekent concreet dat de wet niet exact voorschrijft wat wel en niet mag, maar dat de wet kaders stelt op basis van bepaalde principes. De beleidsregels geven hieraan enige uitwerking. Hiermee ligt de verantwoordelijkheid bij de betreffende bedrijven, overheden en andere organisaties om op basis van de wet een eigen invulling te geven. De IT-auditor dient dus een eigen interpretatie en afweging te maken in overleg met het verantwoordelijk management. De Autoriteit Persoonsgegevens heeft een toezichthoudende rol op onder andere de toepassing van de Wet bescherming persoonsgegevens. Vanuit deze rol heeft zij beleidskaders opgesteld die door organisaties en auditors gebruikt kunnen worden bij hun interpretatie.
- Om te kunnen voldoen aan de meldplicht datalekken treffen bedrijven, overheden en andere organisaties passende beveiligingsmaatregelen. Deze zijn in te delen in maatregelen om te:
  - Voorkomen: een datalek wordt voorkomen door zicht te hebben op nut en noodzaak van een verwerking van persoonsgegevens. Daarnaast is risicomanagement nodig om te bepalen wat passende beveiligingsmaatregelen zijn;
  - Detecteren: signaleren dat een datalek heeft plaatsgevonden. De organisatie zal maatregelen moeten treffen om vast te stellen dat een inbreuk op de beveiliging heeft plaatsgevonden;
  - Beperken: als een datalek plaatsvindt dient de organisatie zo snel mogelijk het lek te dichten en acties te nemen om het verlies van data en de gevolgen voor de individuen en de organisatie te beperken. Vervolgens zal via een efficiënt proces het datalek geregistreerd, beoordeeld, afgewogen en gemeld dienen te worden.
  - Corrigeren: Nadat het lek is gedicht zijn er maatregelen ingericht om te leren van bestaande datalekken en het stelsel van maatregelen te verbeteren.
  - Herstellen: nadat het lek heeft plaatsgevonden worden maatregelen getroffen die eventuele negatieve gevolgen voor het individu verhelpen. Hierbij kan bijvoorbeeld gedacht worden aan (tijdelijke) kredietmonitoring of intensievere monitoring van loggings.
- Bij de impactbepaling van tekortkomingen in de beveiligingsmaatregelen dient de IT auditor zich rekenschap te geven van de boetebepalingen die op kunnen lopen tot € 820.000,- voor onder andere:
  - Ontbreken rechtmatige grondslag;
  - Onverenigbaar gebruik;
  - Langer bewaren dan noodzakelijk;

- Bovenmatig verwerken;
- Geen passende beveiligingsmaatregelen.

- De boetes gelden direct bij opzettelijkheid en ernstig verwijtbare nalatigheid. In alle andere gevallen geldt de boete als na aanwijzing van de toezichthouder de organisatie niet binnen een gestelde termijn de aanwijzing heeft opgevolgd.
- In het kader van de jaarrekeningcontrole bestaat het risico dat de aangepaste boetes een materiële impact hebben. Het verdient aanbeveling dat de IT-auditor dit in dat geval, onderdeel maakt van de IT controle aanpak teneinde dit risico te mitigeren tot een acceptabel risico.
- De privacy wetgeving is principe gebaseerd. Dat heeft tot gevolg dat het verantwoordelijk management zich aan de geldende regelgeving (lees beleidsregels) moet houden dan wel moet uitleggen waarom zij ervan is afgeweken (comply or explain).
- Het verdient aanbeveling van de meldingen zoals bij de Autoriteit Persoonsgegevens een register bij te houden waarin de overwegingen voor de melding worden vastgelegd.