Meldplicht datalekken

Met ingang van 1 januari 2016 is de Wet meldplicht datalekken en de uitbreiding bestuurlijke boetebevoegdheid CBP van kracht. De wet wijzigt de Wet bescherming persoonsgegevens op twee punten: boetebevoegdheid en meldplicht. De wet heeft betrekking op die beveiligingsincidenten waarbij persoonsgegevens verloren zijn gegaan of waarbij we onrechtmatige verwerking van persoonsgegevens niet redelijkerwijs kunnen uitsluiten.

De OU verwerkt persoonsgegevens van onder meer studenten, medewerkers, leveranciers en doet onderzoek met natuurlijke personen en verwerkt daar persoonsgegevens bij. Indien persoonsgegevens kunnen worden ingezien door personen die daarvoor niet geautoriseerd zijn, is er sprake van een datalek. Onder de nieuwe wet is de OU in zo'n geval verplicht om het datalek onverwijld te melden bij de Autoriteit persoonsgegevens. Indien de OU dat na zou laten, kan de Autoriteit persoonsgegevens aan de OU forse boetes opleggen.

Communicatie over datalekken met de pers (ook als de OU door de pers wordt benaderd) vindt uitsluitend plaats door de Woordvoerder OU.

Melden

1. Om wetsovertreding en boetes te voorkomen is het van belang dat medewerkers die een datalek ontdekken, vermoeden of daarover informatie van buiten ontvangen, dat zo snel mogelijk melden bij onze Servicedesk.
2. De Servicedesk zal de melding registreren en ter behandeling door leiden naar de Functionaris gegevensbescherming (FG, en de Security officer (SO , bij afwezigheid).
3. De FG en de SO nemen zo snel mogelijk contact op met de melder om nadere informatie over het incident te verzamelen. Indien het vermoeden bestaat dat informatie over het datalek al breed bekend is buiten de OU, wordt de Woordvoerder OU meteen geïnformeerd.
4. Indien de FG en de SO niet kunnen uitsluiten dat er inderdaad sprake is van een datalek, informeren zij de directeur GSO en de Informatiemanager. De directeur GSO wijst een coördinator voor een onderzoeksteam aan. Deze coördinator stelt een onderzoeksteam samen waarin alle vereiste competenties voor verder onderzoek aanwezig zijn.
   Indien de melding geen datalek blijkt te betreffen, wordt ze verder als informatiebeveiligingsincident afgehandeld door CERT OU.
5. De coördinator start een onderzoek om vast te stellen: hoe het datalek is ontstaan, welke informatie het betrof, welke betrokkenen hierdoor geraakt zijn etc.. Zo nodig wordt hierbij de hulp ingeroepen van het Nationaal Cyber Security Centrum. Zo mogelijk/nodig wordt het lek meteen gedicht.
   De coördinator is gemandateerd om maatregelen te treffen die nodig zijn om verdere onrechtmatige verwerking van persoonsgegevens te voorkomen, inclusief maar niet beperkt tot, het doen uitschakelen van informatiesystemen of onderdelen van de ICT-infrastructuur.
6. De FG maakt op basis van de informatie van de melder en de resultaten van het onderzoek een afweging of het incident als datalek gemeld dient te worden aan de Autoriteit persoonsgegevens en misschien aan (de) betrokkene(n).
7. Indien de FG van mening is dat er sprake is van een datalek dat gemeld moet worden, neemt de coördinator contact op met het CvB. Het CvB beslist of er een melding bij de Autoriteit persoonsgegevens wordt gedaan. Indien wordt besloten om een melding bij de Autoriteit persoonsgegevens te doen, wordt de Woordvoerder OU in het proces betrokken. De FG doet de melding bij de Autoriteit persoonsgegevens.