AVG voor medewerkers

1.0 Voorkomen van datalekken

Een datalek is een inbreuk op de beveiliging waardoor persoonsgegevens verloren gaan of ‘in handen kunnen komen van derden die geen toegang tot die gegevens mogen hebben’. Voorbeelden hiervan zijn:

- Verlies van een usb-stick, laptop als hier persoonsgegevens op staan van b.v. gegevens van studenten of me-dewerkers of relaties.
- Verlies van een smartphone. Een telefoon geeft toegang tot veel informatie waaronder mogelijk gesynchroni-seerde e-mail van school, notities, automatische inlog in systemen. Dit kan zowel bij een bedrijfstelefoon als een privé telefoon.
- ‘Offline’ datalekken; denk hierbij aan papier in de papierbak, studenten verslagen op het bureau, dossiers in de schoudertas.
- Een privé computer, tablet, smartphone thuis, die gehackt of gestolen wordt en waarop b.v. een Excel bestand of mail met gegevens van studenten of medewerkers staan.
- Gehackte (incl. Ransomware ook wel Gijzelsoftware genoemd) bestanden, of inbraak in een databestand.
- E-mail met persoonsgegevens verstuurd naar de verkeerde persoon of aantal personen.

1.1 Preventie

De AVG schrijft voor dat organisaties passende ‘technische en organisatorische maatregelen’ moet nemen om persoonsgegevens te beschermen. Hieronder vallen ook maatregelen om de kans op datalekken te verminderen. ROC College zoekt de oplossing niet in de factor meer (meer geld, meer techniek, meer personeel dat toezicht houdt) maar in de factor slim. We moeten dit samen, slim, oppakken zodat datalekken voorkomen worden. Documenten die door medewerkers worden gemaakt en gedeeld met behulp van Office 365 (e-mail, Word, Excel, PowerPoint) beschouwt ROC College als werkdocumenten. Studenten hebben het recht om alle informatie die over hen gaat of waarin ze genoemd worden, in te zien als zij daarom vragen (Rechten van de Betrokkenen).

Alleen persoonlijke aantekeningen zijn hiervan uitgezonderd: documenten die niet door anderen zijn in te zien of (kunnen) worden gedeeld. Indien de mailbox van medewerkers van ROC College wordt gebruikt voor persoonlijke communicatie, dan moet de medewerker deze mail in een aparte map ‘privé’ plaatsen. Het kan daarbij bijvoorbeeld gaan om communicatie over het eigen functioneren.

Ook privé georiënteerde bestanden kunnen in de eigen OneDrive in een map met privé worden opgeborgen. Als de organisatie dan om motiverende reden (zoals langdurige ziekte, beëindigen dienstverband) noodzakelijke wijze gegevens nodig blijkt te hebben uit de mailbox en/of OneDrive kan in deze bestanden, met medewerking van een ICT medewerker, onder 2 paar ogen principe, noodzakelijk data worden ingezien en/of veiliggesteld waarbij ROC College de zekerheid geeft dat niet in de map met privé in de naam gekeken gaat worden.

1.2 Praktische tips

Om datalekken te voorkomen een aantal tips:

- Sla documenten en bestanden alleen op in veilige omgevingen (R/M drive, Sharepoint, SURFdrive, etc.).
  Sla dus geen bestanden lokaal op je laptop of notebook op. Als je je laptop verliest dan kan de "vinder" de harde schijf eruit halen en zijn alle documenten beschikbaar.
- Voorzie vertrouwelijke Word en Excel documenten van een wachtwoord;
- Als je grote bestanden wilt verzenden gebruik dan niet WeTransfer maar SURFfilesender;
  Zie ook: https://www.surffilesender.nl/
- Verstuur geen bestanden als bijlage in de mail maar verwijs naar veilige omgevingen;
- Zorg dat op je bureau opruimt (clean desk) zodat geen persoonsgegevens rondslingeren;
- Laat geen documenten bij de printer liggen;
- Sluit je scherm af als je wegloopt (clean screen), dit gaat het snelste via de Windows toets linksonder ingedrukt houden en op de [L] drukken;
- Verstuur vergaderverzoeken middels exchange en voeg alle bestanden toe aan het vergaderverzoek;
- Voorzie je laptop van een complex maar goed te onthouden wachtwoord.
- Laat de service desk Bitlocker installeren op je laptop (dit wordt bij nieuwe uitgiften al gedaan).

Als we ons aan deze "slimme" afspraken houden dan hoeft het verlies van een laptop niet tot een datalek te leiden en dus ook niet tot financiële claims van de Autoriteit Persoonsgegevens. Wellicht een overbodige opmerking, de 'Avg politie agent' is niet de FG van ROC College, de privacy officer of de leidinggevenden maar de studenten, medewer-kers en relaties die een beroep doen op hun rechten. Zij kunnen klachten indienen over, bijvoorbeeld, het ontbreken van de benodigde Verwerkersovereenkomsten of gegevens over hen die niet veilig worden opgeslagen.

1.3 Gebruik usb-stick

Het gebruik van een usb-stick lijkt soms handig om bestanden mee naar huis te nemen of even door te geven aan collega's. Maar het gebruik van usb-sticks kent ook grote risico's. Zo wordt er geen backup gemaakt van de bestanden en is verlies niet uit te sluiten. En als er ook een studentenlijst of andere persoonsgegevens op staan zal het verlies van een usb-stick altijd gemeld moeten worden als mogelijk datalek via de FG. Dit zijn enkele redenen waarom het gebruik van een usb-stick wordt afgeraden. Gebruik je toch een usb-stick, zorg er dan voor dat alle bestanden op de usb-stick 'versleuteld' zijn. (Encryptie, b.v. met BitLocker onder Windows10).

1.4 Mail naar teveel of een verkeerd adres

Vaak worden mailtjes verstuurd met meerdere e-mailadressen in de **[Aan]** en **[CC]**.
Doordat dit soort mailtjes ook wel eens doorgestuurd worden naar privé mailadressen is dit niet alleen onwenselijk vanuit privacy maar ook onwenselijk vanuit informatiebeveiliging.
Plaats het liefst één geadresseerde in de 'Aan' en plaats overige email adressen in de **[BCC]**

In de eerste tekstregel kun je dan aangeven:

Dit mailtje is in copy verstuurd naar:
Naam1, Naam2, … (*en dus geen email adressen*)

Stuur je een bulk mailtje:

Stuur het mailtje aan jezelf en zet alle emailadressen in de **[BCC]**

Als in één van deze gevallen het mailtje in verkeerde handen terechtkomt gaat het maar om hooguit één emailadres. Het kan ook voorkomen dat er per ongeluk een mail naar een verkeerd emailadres (lijst) gestuurd wordt. In dat geval stuur meteen een mail er achteraan met het verzoek om het vorige mailtje te verwijderen. Je bent dan wel afhankelijk van de goede wil van die andere.

Meldt dit tevens bij gevoelige bedrijfsgegevens of privacy gegevens bij de service desk als incident en bij privacy@roccollege.nl. Er kan dan nagegaan worden of er nog meer stappen ondernomen moeten worden