Tips & tricks AVG-proof werken bij de klant

Je hebt bij de klant toegang tot (een deel van) belangrijke persoonsgegevens. Het is daarom van belang dat iedereen zich bewust is van de informatie van personen die wordt verzameld, gebruikt en vernietigd. Wij willen daarom met nadruk vragen om altijd zorgvuldig om te gaan met persoonsgegevens. Hoe je dat doet? Onderstaand lees je enkele tips.

1. **Vergrendel de computer als je even wegloopt**
   Het is mogelijk dat er veel privacygevoelige informatie te vinden is op de computers bij de klant. Mocht je van je plek lopen, al is het even naar de printer, vergrendel altijd de computer. Zo kunnen onbevoegden geen toegang krijgen tot belangrijke persoonlijke gegevens.

2. **Check e-mails op echtheid**
   Er komen regelmatig phishing-aanvallen bij bedrijven voorbij: de afzender probeert bijvoorbeeld iemand te verleiden om te klikken op een valse websitelink, waar iemand gevoelige informatie moeten prijsgeven. Hierdoor krijgt de fraudeur beschikking over persoonlijke gegevens. Hoe je een phishing-aanval kan voorkomen? Check e-mails op echtheid:

   - Een phishing-mail heeft geen persoonlijke aanhef, maar begint met een algemene opening, zoals: ‘Beste meneer’;
   - Er staan vaak veel taal- en spellingsfouten in de mail;
   - Er wordt gesuggereerd dat het account geverifieerd moet worden met inloggegevens;
   - Er wordt gedreigd met gevolgen als er geen gehoor wordt gegeven aan de mail;
   - De websitelink wijkt af van de naam van de oorspronkelijke website.

3. **Clean Desk Policy**
   Clean Desk Policy voorkomt dat vertrouwelijke informatie wordt gelezen of meegenomen door interne fraudeurs. Het verkleint de kans op informatiediefstal, fraude en beveiligingslekken.

   Houd je bureau opgeruimd en laat geen bedrijfsdocumenten, notities of bijvoorbeeld namen van bezoekers rondslingeren. Tevens is het van belang aan het eind van de werkdag alle documenten veilig op te bergen en computers uit te schakelen.

4. **Gebruik voor elk systeem een ander wachtwoord**
   Het is aan te raden om voor elk systeem een ander wachtwoord te gebruiken. Het is makkelijker om één wachtwoord te hebben voor meerdere websites, maar als eenmaal één wachtwoord is gekraakt, dan is er direct toegang tot meerdere websites waar je gebruik van maakt.

   Het is natuurlijk lastig om alle wachtwoorden te onthouden, maar hiervoor zijn diverse wachtwoordmanagers ontwikkeld. Dit zijn beveiligde hulpmiddelen om de wachtwoorden op te slaan. Via Google kan je tips vinden voor het gebruik van een wachtwoordmanager.

   Tevens is het aan te raden ‘sterke’ wachtwoorden te gebruiken: een wachtwoord van minimaal 8 tekens met gebruik van letters, cijfers en symbolen. Gebruik geen voor de hand liggende informatie zoals naam, adres en geboortedatum. Verander tevens regelmatig je wachtwoord.

5. **E-mail goed nalezen**
   E-mail is één van de meest gebruikte communicatiemethoden binnen organisaties, maar tegelijkertijd ook een foutgevoelige methode. In de snelheid stuurt iemand per ongeluk een e-mail naar de verkeerde persoon of worden er onnodig mensen in de CC meegenomen, waardoor er meer mensen dan nodig toegang hebben tot persoonsgegevens. Goed om te weten is dat dit al wordt gezien als een data-lek. Check daarom voor verzenden altijd goed of de e-mail naar de juiste medewerkers gaat.

Tot zo ver een aantal tips omtrent de AVG. Mocht je naar aanleiding van dit document nog vragen hebben, neem dan gerust contact op met onze afdeling Backoffice via backoffice@trinitybv.nl.