Protocol voor datalek AVG regelgeving

Dit protocol maakt onderdeel uit van het totale beleid van ons kantoor en meer specifiek het beleid ten aanzien van bescherming van persoons- en privacy gevoelige gegevens, e.e.a. zoals verwoord in de AVG.

BalvertAdviseurs Finance & Tax stelt vast of sprake is van een datalek. Hiertoe worden de volgende stappen doorlopen:

1. Is de AVG en daarmee de meldplicht van toepassing?

Meer concreet houdt dit in dat vastgesteld zal moeten worden of de AVG van toepassing en of er sprake is van verwerking van persoons- en/of andere privacy gevoelige gegevens.

a. Persoons- of privacy gevoelige gegevens in het geding?
b. Zijn deze gegevens geheel of gedeeltelijk geautomatiseerd verwerkt?
c. Zijn deze gegevens bedrijfsmatig verwerkt?

2. Is sprake van een datalek?

Er is alleen sprake van een datalek als zich daadwerkelijk een beveiligingsincident heeft voorgedaan, waarbij persoonsgegevens verloren zijn gegaan of als onrechtmatige verwerking van de persoonsgegevens niet kan worden uitgesloten.

d. Heeft beveiligingsincident plaatsgevonden (zie voor voorbeelden verder in protocol)?;
e. Zo ja, zijn hierbij persoonsgegevens betrokken geweest?
f. Zo ja zijn deze verloren gegaan of heeft onrechtmatige verwerking plaatsgevonden, danwel kan het risico hierop niet worden uitgesloten?

3. Melden datalek bij Autoriteit Persoonsgegevens

BalvertAdviseurs Finance & Tax moet (systematische) inbreuken op de privacy signaleren. Onze organisatie is daartoe in staat door middel van het door haar geformuleerde beleid. Hierin is o.a. opgenomen dat periodiek gemonitored en geëvalueerd wordt ten aanzien van haar beveiligingsbeleid.
Indien een inbreuk heeft plaatsgevonden en er is sprake van (een aanzienlijke kans op) nadelige gevolgen voor betrokkenen, dan zal BalvertAdviseurs Finance & Tax overgaan tot melding aan de Autoriteit Persoonsgegevens.

Een melding wordt binnen 72 uur nadat wij hiervan kennis hebben genomen gemeld aan de Autoriteit Persoonsgegevens, e.e.a. zonder onredelijke vertraging. Indien vertraging mocht ontstaan en de melding niet binnen 72 uur plaatsvindt zullen wij de reden van vertraging melden.

Een melding dient plaats te vinden indien persoonsgegevens van gevoelige aard zijn gelekt. Een melding is niet noodzakelijk als het niet waarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

De feitelijke melding zullen wij doen door gebruik te maken van het meldingsformulier, e.e.a. zoals beschikbaar op de website van de Autoriteit Persoonsgegevens.

https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?1

De melding dient de volgende gegevens te bevatten:

1. Aard van de inbreuk;
2. Omvang van de inbreuk;
3. Mogelijke gevolgen van de inbreuk;
4. Maatregelen die zijn genomen na de inbreuk;

Ook indien wij optreden als verwerker van gegevens en wij constateren een inbreuk, dan stellen wij de verwerkingsverantwoordelijke zo snel mogelijk hiervan op de hoogte. In ons geval kan dat inhouden dat wij een inbreuk bij een cliënt constateren. Zowel cliënt als onze organisatie is dan gehouden de AVG te volgen hetgeen in ons geval inhoudt dat wij dit protocol onverkort zullen volgen.

Wij zullen monitoren of de verwerkingsverantwoordelijke zijn/haar plicht nakomt tot het melden van het datalek aan de Autoriteit Persoonsgegevens. Indien wij vaststellen dat dat niet het geval is zullen wij diegene aansporen, doch bij uitblijven van enige actie zullen wij zelf de melding doen bij de Autoriteit.

4. Informeren betrokkene(n) over datalek

Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk risicovol is voor de rechten en vrijheden van natuurlijke personen, dan brengen wij de betrokkene(n) direct op de hoogte van de inbreuk. Dit ter voorkoming van ernstige schade bij betrokkenen als gevolg van het verlies, onrechtmatig gebruik of misbruik van hun persoonsgegevens.

Voorbeelden van mogelijke beveiligingsincidenten

1. Iemand heeft oneigenlijk toegang verkregen tot data, bijvoorbeeld door een hack op ons systeem, nb phishing en malware hiermee gelijk gesteld;
2. NB hetgeen vermeld onder punt 1 kan zich ook voordoen bij een van onze subverwerkers, zoals Kleisteen, Twinfield of KBP aangiftesoftware, danwel onze cloud-leverancier t.b.v. backup Microsoft;
3. Onze organisatie is een USB-stick kwijtgeraakt of deze is ontvreemd en daarop stond relevante data;
4. Er is ingebroken bij onze organisatie en de server met data is ontvreemd;
5. De laptop van onze organisatie is ontvreemd en daarop stond relevant data;
6. Onze organisatie is een telefoon kwijtgeraakt of deze is ontvreemd en daarop stond relevante data;
7. Onze organisatie heeft een email met relevante data abusievelijk verzonden naar de verkeerde geadresseerde;

8. Buiten gebruik gestelde ICT apparatuur bevat nog relevante data;
9. Vorenstaande geldt mutatis mutandis ook voor papieren data

Protocol van kracht dd. 25-5-2018