DataSpeed Protocol meldplicht datalekken

DataSpeed wenst haar klanten, de gebruikers van [gevoelige] persoonsgegevens, bewust te maken van de veranderde wetgeving op het gebied van bescherming persoonsgegevens. Zo is op 1 januari 2016 een belangrijke wijziging in de wetgeving doorgevoerd, namelijk de meldplicht datalekken.

Wat is een datalek?
Een datalek is een inbreuk op de beveiliging die leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van, of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens. Die inbreuk kan per ongeluk zijn: één van de medewerkers mailt bijvoorbeeld een bestand met persoonsgegevens aan een verkeerde ontvanger, of door een verkeerde instelling zijn vertrouwelijke klantgegevens toegankelijk voor alle bezoekers van de website. De inbreuk kan ook met opzet gebeuren: een hacker maakt bijvoorbeeld persoonsgegevens buit, of een medewerker neemt een kopie van een database met persoonsgegevens mee.

Meldplicht
De meldplicht houdt in dat men **binnen 72 uur** een melding moet doen bij de Autoriteit Persoonsgegevens indien zich een datalek heeft voorgedaan. Dit geldt zowel voor DataSpeed , bijvoorbeeld in geval van een inbraak door een hacker op onze cloudserver[s]; een malware-besmetting of een calamiteit zoals een brand in een datacentrum alsook voor u als klant/gebruiker van ons presentie- en absentieregistratiesysteem Ipas. Niet elk datalek hoeft te worden gemeld. Of een datalek gemeld dient te worden ligt, in overleg met de directie, ter beoordeling bij de functionaris gegevensbescherming. Volgens de wetgeving dienen u ieder datalek te melden wanneer er sprake is van een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens.

In bepaalde gevallen dient een datalek niet alleen aan de Autoriteit Persoonsgegevens gemeld te worden, maar ook aan de personen van wie de persoonsgegevens gelekt zijn (de betrokkenen). Deze meldplicht geldt als de inbreuk waarschijnlijk ernstige nadelige gevolgen zal hebben voor de persoonlijke levenssfeer van betrokkene.

Bij een overtreding van de meldplicht datalekken kan de Autoriteit Persoonsgegevens een hoge boete opleggen. Deze boetes zijn een grote kostenpost, maar veel belangrijker is dat de opgelegde boete kan leiden tot grote imagoschade voor uw instelling. Per 25 mei 2018 kunnen bij niet (volledige) naleving van de AVG boetes worden opgelegd oplopend tot wel 20 miljoen euro of 4% van de wereldwijde jaaromzet van de betreffende organisatie.

Wij binnen DataSpeed hebben de privacy hoog in het vaandel staan en wij profileren ons zowel intern als extern ook als een organisatie die zeer zorgvuldig om gaat met persoonsgegevens. Het is daarom van groot belang dat elk beveiligingsincident serieus wordt genomen en dat hier adequaat op wordt gereageerd.

Onze en uw medewerkers dienen zich bewust te zijn van het belang van een adequate beveiliging van persoonsgegevens. Zij dienen bij de uitoefening van hun werkzaamheden hiermee zorgvuldig om te gaan.

In dit protocol wordt weergegeven welke stappen er genomen dienen te worden wanneer een datalek heeft plaatsgevonden.

Criteria voor een datalek
Alleen datalekken die voldoen aan de volgende drie criteria dienen gemeld te worden bij de Autoriteit:

1. De verwerkte persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking;

   De Autoriteit Persoonsgegevens noemt de volgende voorbeelden:
   - een kwijtgeraakte USB-stick;
   - een gestolen laptop;
   - inbraak door een hacker;
   - verzending van een e-mail waarin de e-mailadressen van alle geadresseerden zichtbaar zijn voor alle andere geadresseerden;
   - een malware-besmetting;
   - het kwijtraken van persoonsgegevens op papier of het verzenden naar het verkeerde adres;
   - een calamiteit zoals een brand in een datacentrum.

2. Er kan redelijkerwijs vanuit worden gegaan dat persoonsgegevens verloren zijn gegaan of onrechtmatig zijn verwerkt (of ingezien).

   Bijvoorbeeld:
   - er zijn geen backups van de bestanden die verloren zijn gegaan bij een brand;
   - er is bewijs dat gegevens zijn bewerkt (of ingezien) door onbekende derden.

3. Er is sprake van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens.

   Bijvoorbeeld:
   - er zijn persoonsgegevens van gevoelige aard gelekt;
   - de aard en omvang van de inbreuk leiden tot (een aanzienlijke kans op) ernstige nadelige gevolgen, zoals bijvoorbeeld identiteitsfraude, diefstal of reputatieschade.

Melden aan de Autoriteit Persoonsgegevens
Wij begrijpen dat het lastig is om in te schatten wanneer sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Gelet hierop is het de werknemer van DataSpeed danwel een medewerker/gebruiker van de klant niet toegestaan zelf een afweging te maken of sprake is van een datalek die gemeld moet worden en dient elk beveiligingsincident, datalek of het vermoeden hiervan in overleg met de directie te worden gemeld bij de functionaris gegevensbescherming. De functionaris gegevensbescherming zal vervolgens de afweging maken of het datalek gemeld moet worden.

Acties bij een (mogelijk) datalek
Om voor een ieder duidelijk te maken hoe te handelen bij een datalek is een stappenplan opgesteld:

Stappen	Acties	Wie
1	Meld een beveiligingsincident, of bij een vermoeden hiervan, **direct, dan wel uiterlijk binnen 12 uur na ontdekking van een beveiligingsincident,** aan de functionaris gegevensbescherming binnen uw instelling danwel aan DataSpeed	Degene die het beveiligingsincident heeft ontdekt
2	Vul onderstaand, intern meldingsformulier in	Degene die het beveiligingsincident heeft ontdekt
3	De functionaris gegevensbescherming gegevensbescherming, binnen uw instelling danwel binnen DataSpeed, zal contact opnemen met de melder om een totaalbeeld van het beveiligingsincident te melden.	functionaris gegevensbescherming, binnen uw instelling danwel binnen DataSpeed
4	functionaris gegevensbescherming, binnen uw instelling danwel binnen DataSpeed, zal in overleg met directie, de procedure in gang zetten.	functionaris gegevensbescherming. binnen uw instelling danwel binnen DataSpeed
5	Evalueer ieder datalek om te kijken of er verbeteringen mogelijk zijn en voer deze door.	en degene die het beveiligingsincident heeft ontdekt

Meldingsformulier
Het meldingsformulier dient altijd volledig te worden ingevuld en dient **binnen 12 uur** bij de functionaris gegevensbescherming ingediend te zijn. Immers DataSpeed dan wel uw instelling moet voldoende tijd en gelegenheid krijgen om een afweging te maken of zij binnen 72 uur na ontdekking van een beveiligingsincident - of het vermoeden hiervan - een melding dient te doen bij de Autoriteit Persoonsgegevens. De termijn van 72 uur begint al te lopen op het moment dat u bekend bent geraakt met een beveiligingsincident/datalek of het vermoeden hiervan.

Handhaving
DataSpeed treft disciplinaire maatregelen indien een medewerker zich niet aan de in dit reglement opgenomen bepalingen houdt. DataSpeed gaat ervan uit dat u, als klant zijnde, ook de de nodige disciplinaire maatregelen hierin zal nemen jegens uw medewerker[s] binnen uw eigen instelling/organisatie indien deze zich niet aan de in dit reglement opgenomen bepalingen houdt.

Intern meldingsformulier:

Naam:	
Contactgegevens:	
Datum en tijdstip ontdekking:	
Datum, tijdstip en locatie van het incident/lek:	
Op welke informatie/persoonsgegevens heeft het incident/lek betrekking:	
Beschrijving van hoe het incident/lek is ontdekt;	
Beschrijving waarop het incident/lek betrekking heeft (bijvoorbeeld op een apparaat, een papieren document etc.)	
Datum en tijdstip melding bij functionaris gegevensbescherming:	
Overige informatie:	