AVG – Afspraken

1.AVG en onderwijs

Deze leidraad is bedoeld om je te helpen voldoen aan de Algemene Verordening Gegevensbescherming (AVG) en biedt concrete voorbeelden. De leidraad is niet allesomvattend maar geeft je een goed idee van de processen en factoren waarmee je vanaf 25 mei 2018 rekening dient te houden, de datum waarop de AVG is ingegaan. De AVG is van toepassing op onderwijsinstellingen en organisaties in Europa.

De vereisten van de AVG omvatten fysieke beveiliging, netwerkbeveiliging, beveiliging van opslag en computers, identiteitsbeheer, toegangscontrole, versleuteling en risicobeperking.

2. Wat zijn persoonsgegevens?

Met persoonsgegevens bedoelen we alles wat herleidbaar is naar een persoon, wat van een mens een mens maakt. Dat is een naam maar ook een foto (NAW, geboortedatum, stem/bandopname, foto, telefoonnummer, IP-adres, IMEI enzovoort). Bijzondere persoonsgegevens zijn het BSN, godsdienst of levensovertuiging, medische gegevens (maar ook bijvoorbeeld dyslexie).

Zodra je persoonsgegevens vastlegt en ergens voor gebruikt is de AVG van toepassing. Dat gebeurt in alle lagen van het onderwijs. Denk aan leerlingvolgsysteem, voortgangsrapportages, klassenlijsten maar ook aan de foto's op Facebook van een sportdag, musical.

Kinderen zijn een kwetsbare groep. Met de komst van steeds meer digitale mogelijkheden en sociaal media wordt privacy steeds belangrijker.

Je moet als school vastleggen waarvoor je de verzamelde gegevens gebruikt. Weet waarom je die gegevens nodig hebt en houdt dat ook bij. Die documentatieplicht weegt zwaar.

3. Wat voor impact heeft de AVG?

a. De AVG versterkt de gegevensbescherming *voor medewerkers, ouders en leerlingen en geeft hen het recht om:*

- gegevens in te zien en onnauwkeurigheden te corrigeren; (met een wachttijd van max een week)
- gegevens te wissen;
- bezwaar te maken tegen de verwerking van hun gegevens;
- hun gegevens te verplaatsen.

b. Meldplicht voor datalekken

Onderwijsinstellingen dienen datalekken binnen 72 uur te melden bij de Functionaris gegevensbescherming (via privacy@fluenta.nl).

c. Hoge boetes voor inbreuk

Onderwijsinstellingen riskeren hoge boetes als ze niet voldoen aan de wet AVG.

4. De Functionaris Gegevensbescherming

Fluenta heeft een Functionaris Gegevens bescherming (FG) aangesteld in de persoon van mevrouw Marion van der Horst (CED-Groep). Daarnaast heeft Fluenta een Security Officer (SO). Dit is Dick van Oostenbruggen (Stichting Fluenta).
Alle datalekken dienen bij de SO te worden gemeld. Dit kan via het e-mailadres: privacy@fluenta.nl.

5. Voorbeelden van datalekken

- De papierbak (gebruik een versnipperaar bij privacygevoelige gegevens).
- Verloren USB-sticks (met persoonsgegevens).
- Verloren telefoon (privé en zakelijk).
- Gestolen laptop (privé en zakelijk).
- Hacking.
- Malware en phishing.
- Verkeerd verzonden e-mail.
- Post.
- De menselijke fout. Het kan ons allemaal gebeuren. Belangrijk hierin is dat het **altijd** wordt gemeld bij privacy@fluenta.nl.

Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens maar ook onrechtmatige verwerking van gegevens.

6. Privacy: zo ga je daarmee om!

Praktische tips

- **De klassenmap:** laat je klassenmap met persoonlijke gegevens van leerlingen nooit onbeheerd achter (achter slot en grendel of de klas op slot als je even weg gaat).
- Opgeruimde werkplek: laat geen documenten op je bureau liggen en hang geen lijstjes met NAW-gegevens op in de klas of in de teamkamer.
- Leerlingdossiers achter slot en grendel of kantoor/klas op slot. (alles zoveel mogelijk in ParnasSys)
- Schermvergrendeling: leer jezelf en je leerlingen aan om het scherm te vergrendelen (Windows teken + L). **Verlaat je je lokaal: vergrendel je scherm!**
- Gebruik beeldmateriaal: plaats alleen foto's en video's van leerlingen en medewerkers op de media waarvoor schriftelijk en ondubbelzinnig toestemming voor is gegeven. Denk ook aan de WhatsAppgroepen **(toestemmingsformulier).**
- Wees zuinig met wat je deelt. Ouders mogen altijd inzage vragen in leerlinggegevens van hun kinderen. Medewerkers mogen inzage vragen in al hun eigen gegevens.
- Printen: print zo min mogelijk en laat geen vertrouwelijke documenten bij de printer liggen.
- Weggooien gegevens: in een "vertrouwelijke kliko".
- Contactgegevens ouders: een ouder vraagt om contactgegevens van een andere ouder. Vraag eerst toestemming aan de desbetreffende ouder voordat je gegevens deelt.
- Meekijken: zorg dat er niemand kan meekijken wanneer je inlogt of een toepassing open hebt staan met daarin persoonsgegevens.
- Gebruik geen USB-sticks. Opslaan in Google Drive.
- Noodlijsten: alleen naam en noodnummer. – in ons geval niet: gebruik Parro – P – app.
- **Zet e-mailadressen altijd in de bcc**
- Als laatste nogmaals: heb je een datalek (telefoon kwijt, e-mail verkeerd verzonden: stuur een e-mail naar privacy@fluenta.nl
- Speciale website waar alles terug te vinden is: https://sites.google.com/fluenta.nl/avg-privacy-fluenta/homepage