GIPS Spelen & Leren
Privacy beleid en protocollen

Inleiding
In het kader van de wetgeving over de bescherming van persoonsgegevens is dit beleid en protocol vastgesteld. GIPS S&L wilt transparant en conform de wetgeving met persoonsgegevens om gaan. Welke uitgangspunten gehanteerd worden en hoe dat geregeld is binnen de organisatie wordt in dit document beschreven.

Definities
Data-lek: er is sprake van een data-lek als persoonsgegevens per ongeluk en/of onrechtmatig verspreid of vernietigd of gewijzigd worden of verloren gaan als gevolg van een beveiligingsprobleem;
Ex-medewerker: dit betreft oud-medewerkers en mensen die overleden zijn waarvan dit bij GIPS S&L bekend is;
Filemaker (FM): dit is het maatwerk softwarepakket dat door GIPS S&L gebruikt wordt om gegevens van personen te registreren, activiteiten te plannen, activiteiten te factureren, artikelen te bestellen en gegevens m.b.t. wachtwoorden te beheren;
Mac Mini: server waarop de planningssoftware draait en de database opgeslagen is.
Medewerker: dit zijn de vrijwilligers en beroepskrachten;
NAS: externe harde schijf die via het kantoornetwerk en vanaf extern benaderbaar is
Persoonsgegevens: alle gegevens die herleidbaar zijn naar een persoon;
Relaties: dit zijn de leveranciers, klanten, scholen, sponsoren, subsidieverleners en samenwerkingspartners van GIPS S&L.

Welke persoonsgegevens worden bewaard en waarom
Er worden van verschillende personen gegevens bewaard die vanuit verschillende rollen een samenwerking met GIPS S&L hebben. We onderscheiden hierbij:

- Relaties;
- Medewerkers;
- Ex-medewerkers.

Gegevens van relaties
Van relaties worden de volgende gegevens bewaard:

- Naam van de organisatie;
- Naam, functie, telefoonnummers, mailadressen van contactpersonen;
- NAW gegevens (eventueel: bezoek-, lever- en factuuradres);
- Website en evt. social media gegevens.

Deze gegevens zijn van belang om activiteiten af te stemmen die GIPS S&L uitvoert bij relaties en contacten te onderhouden. De gegevens zorgen ervoor dat activiteiten voor en contacten met relaties binnen de organisatie, daar waar dit vereist is, overdraagbaar zijn.

Gegevens van medewerkers

Van medewerkers worden de volgende gegevens bewaard:

- Roep- en achternaam (hiervoor wordt een acroniem aangemaakt);
- Geboortedatum en geslacht;
- NAW-gegevens (woonadres, evt. ophaaladres);
- Telefoon, mailadres;
- Datum start bij GIPS S&L;
- Datum stop bij GIPS S&L met de reden van stoppen;
- Indeling in functie bij GIPS;
- Naam van de beperking en hulpmiddel(en);
- Beschikbaarheid (dagen van de week);
- Afwezigheid (datum met reden);
- Bankrekeningnummer (bij externe boekhouder);
- BSN-nummer (alleen beroepskrachten).

De gegevens van de medewerker zijn nodig om de inzetbaarheid van medewerkers in te kunnen plannen. Medewerkers maken deel uit van een team dat de activiteiten van GIPS bij relaties uitvoert. Er wordt naar gestreefd voldoende variatie aan beperkingen binnen een team vertegenwoordigd te hebben. Daarnaast is het van belang om te weten welke hulpmiddelen gebruikt worden zodat het vervoer van medewerkers effectief gepland kan worden. De omschrijving van de beperking is gebaseerd op de informatie van de medewerker en in algemene termen zonder medische details. Het bankrekeningnummer wordt uitsluitend in de boekhouding gebruikt voor het voldoen van declaraties en salarissen. Deze gegevens zijn opgeslagen in de software van de bank waarmee de betalingen gedaan worden en het boekhoudprogramma.

Bij de intake procedure wordt expliciet gevraagd om de toestemming, de opgenomen gegevens te mogen verwerken bij GIPS S&L. Het privacy statement wordt door de administratie aan de kandidaat medewerker verstrekt (hard copy of elektronisch) bij inschrijving.

VOG

Alle medewerkers die worden ingeschreven wordt verzocht een VOG aan te vragen. Het VOG is een voorwaarde om te mogen werken bij GIPS S&L.

Gegevens van ex-medewerkers

Van medewerkers worden de volgende gegevens bewaard:

- Roep- en achternaam (plus acroniem);
- Geboortedatum en geslacht;
- NAW-gegevens postadres;

- Telefoon, mailadres;
- Soort werkzaamheden bij de stichting;
- Datum start bij GIPS S&L;
- Datum stop bij GIPS S&L met de reden van stoppen.

De gegevens van de ex-medewerker worden bewaard om contacten te kunnen blijven onderhouden daar waar dit gewenst wordt. Dit is bijvoorbeeld voor de toezending van de nieuwsbrieven, uitnodiging voor een reünie, symposium, e.d. Wat **altijd** bewaard zal blijven is de roepnaam, achternaam en het acroniem van een medewerker. Deze is gekoppeld aan de historie van de planning.

Projecten of tijdelijke activiteiten

Voor tijdelijke activiteiten, projecten die eindig zijn etc. kunnen persoonsgegevens van belang zijn. De projectleider dient de afweging te maken in het kader van dit beleid welke gegevens van belang zijn en eventueel gedeeld worden. Van alle participanten wordt verwacht dat na beëindiging van de activiteiten, persoonsgegevens worden verwijderd. Door de projectleider wordt een digitaal archief gemaakt dat via de administratie op kantoor opgeslagen kan worden op de beveiligde omgeving (NAS).

Waar worden persoonsgegevens opgeslagen

Bij GIPS S&L wordt gebruik gemaakt van een aantal systemen voor het opslaan en beheren van persoonsgegevens. Dit zijn de volgende systemen:

- Filemaker, draaiende op de server (mac-mini);
- NAS (externe harde schijf);
- Back up Filemaker bij de programmeur;
- Back up Directie;
- Back up schijf kantoor;
- PC’s en laptops in gebruik op kantoor of door medewerkers van GIPS S&L.

Opslag van persoonsgegevens

Ook hier geldt weer het onderscheid relaties en medewerkers. Gezien de aard van de contacten verschillend is, kunnen gegevens op meerdere manieren opgeslagen worden.

Opslag van gegevens van relaties

De gegevens van relaties worden opgeslagen:

- Filemaker;
- Op laptops of pc’s van medewerkers.

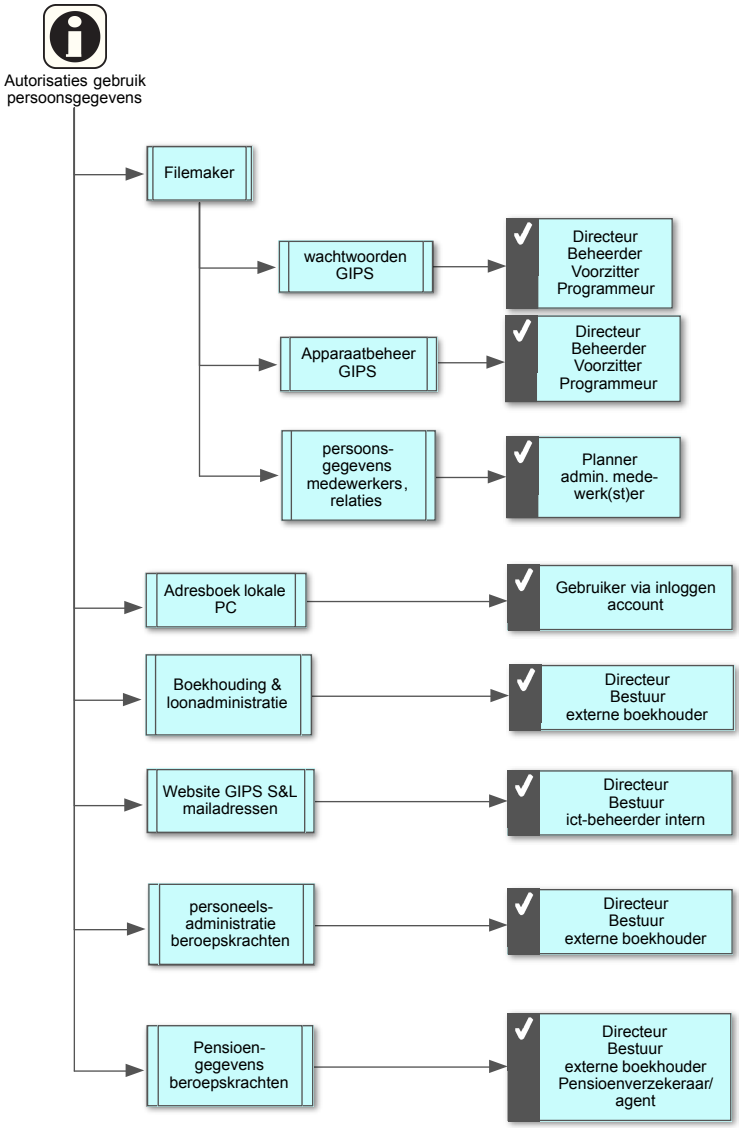
Opslag van gegevens van medewerkers

- Filemaker;
- Op laptops of pc’s van medewerkers exclusief gegevens mits beperkt tot naam, NAW, mail en telefoonnummers;

- In geval van een hard-copy in een afgesloten kast.

Autorisatie beheer en/of gebruik van persoonsgegevens

In onderstaande schema staan de autorisaties weergegeven m.b.t. de persoonsgegevens.



De voorzitter krijgt een verzegelde enveloppe in beheer met de toegangsgegevens waarmee alle wachtwoorden toegankelijk zijn. Tevens zijn hierbij vermeld alle relevante telefoonnummers.

Door externe partners die toegang hebben tot persoonsgegevens moet een verklaring afgegeven worden dat zij voldoen aan de gestelde eisen van de Algemene Verordening Gegevensbescherming – AVG -. Deze verklaringen worden in FM bewaard bij de gegevens van de betreffende relatie.

Hoe worden persoonsgegevens beschermd

Computers en elektronische apparaten

Alle elektronische apparaten waarop persoonsgegevens bewaard worden of toegang verschaffen tot persoonsgegevens, zijn met een wachtwoord beveiligd. Apparaten schakelen na 10 minuten in de schermbeveiligingmodus. Medewerkers hebben hun eigen account en inlognaam waarmee zij op computers van GIPS kunnen inloggen.

Up-dates installeren

Alle door GIPS S&L beheerde apparaten wordt op regelmatige basis gecontroleerd of er up-dates nodig zijn. De gebruiker van het betreffende apparaat dient dit minimaal één keer per 14 dagen te doen. Daar waar automatische meldingen van up-dates gedaan worden dienen deze binnen 1 dag geïnstalleerd te worden. Als een update automatisch aangekondigd wordt dient deze binnen 1 dag uitgevoerd te worden.

Virusscanners

De externe ict-beheerder zorgt er voor dat alle computers voorzien zijn van virusscanners. Hij draagt er ook zorg voor dat deze up-to-date zijn.

Maatregelen om hacken tegen te gaan

De beveiliging van de server, het netwerk van GIPS en het draadloze modem worden centraal beschermd door middel van een professioneel pakket. Inloggen in de planningssoftware gebeurt met een persoonlijke gebruikersnaam en wachtwoord.

Hard-copy

Daar waar sprake is van het archiveren van documenten met persoonsgegevens, gebeurt dit in kasten die afgesloten zijn.

Wachtwoordenbeleid

Wachtwoorden van medewerkers die daarmee toegang hebben tot persoonsgegevens zullen één keer per jaar in Maart gewijzigd worden. De wijzigingen worden vastgelegd in FM. Uitgezonderd hiervan zijn de inloggegevens van het bestuur die in de verzegelde brief opgenomen zijn. De programmeur, die toegang heeft tot de software, volgt zijn eigen beleid en werkwijze in deze met als leidraad de wetgeving.

Privé computers die voor GIPS gebruikt worden

Medewerkers die gebruik maken van privé computers voor het uitvoeren van werkzaamheden voor GIPS S&L en die persoonsgegevens op deze computer bewaren, zijn gehouden aan het volgen van het privacy-beleid van GIPS S&L.

Verstrekken van gegevens intern en extern

Alleen die informatie die functioneel van belang is wordt gedeeld. Dit wordt gedaan als de activiteiten of werkzaamheden van een medewerker hier aanleiding toe geven. Indien een medewerker wenst dat zijn/haar gegevens niet aan derden verstrekt worden, dient hij/zij dit te melden bij de administratie. Bij de intake van een nieuwe medewerker wordt hiernaar gevraagd door de intaker. Dit wordt aangevinkt op het inschrijfformulier.

Persoonsgegevens bescherming op school (leerlingen en leerkrachten)

Bij iedere bevestiging van een opdracht op school wordt een informatie-set t.b.v. van de school (leerkracht) meegestuurd. Daarin wordt aangegeven dat de mogelijkheid bestaat dat foto's of video opnamen gemaakt worden. Indien de school hier bezwaar tegen heeft kan dit vooraf aan het team aangegeven worden. In dat geval zal daar rekening mee gehouden worden. Als een team op school foto's of video opnamen wil maken zullen zij dit bij de leerkracht vooraf melden.

Medewerkers hebben een naam badge met uitsluitend de roepnaam.

Op de ritplanning staan gegevens van de school, leerkracht en teamleden. De ritplanning wordt ingeleverd nadat het project op school is uitgevoerd. Ritplanningen worden maximaal 1 jaar bewaard op kantoor in een afgesloten kast. Daarna worden deze vernietigd.

Medewerkers van GIPS geven in het kader van het project, voornaam plus beperking van elke medewerker aan de leerkracht ter voorbereiding van de tweede sessie van het project. Scholen worden er op gewezen dat zij deze gegevens uitsluitend voor het GIPS project mogen gebruiken.

Inzage in persoonsgegevens

Medewerkers en relaties kunnen opvragen welke gegevens van hem/haar bewaard worden. Op verzoek worden deze toegestuurd.
Als blijkt dat (bepaalde) gegevens niet juist of onvolledig zijn, dan moet GIPS S&L op verzoek van medewerkers en relaties deze gegevens verbeteren en/of aanvullen.

Geheimhouding

Personen die permissie hebben persoonsgegevens (zowel algemeen als bijzondere gegevens) te registreren en raadplegen, zijn verplicht tot geheimhouding tenzij er een wettelijke of redelijke noodzaak toe bestaat gegevens te verstrekken.

Bulkmail

Het begrip bulkmail omvat e-mailberichten of postzendingen. Alle vormen van bulkmail zijn doeltreffende middelen om doelgroepen van GIPS S&L op een directe manier te bereiken. Er is sprake van een bulkmail wanneer deze meer dan 20 unieke geadresseerden betreft. Uitgezonderd zijn projectgroepen, overleggroepen, die in het kader van hun werkzaamheden mails ontvangen. Voor bulkmail berichten geldt dat ontvangers zich kunnen

afmelden Dit wordt dan in FM geregistreerd. Indien er sprake is van bulkmail via de elektronische weg, dan worden de mailadressen in de BCC geplaatst.

Datalekken en wat als er misbruik geconstateerd is

Constateert of vermoedt een medewerker een data-lek of misbruik van persoonsgegevens, dan dient dit onverwijld mondeling en/of schriftelijk gemeld te worden aan de directie. De directie zal samen met de Functionaris Gegevensbescherming de vereiste stappen ondernemen om het data-lek op te heffen.
GIPS S&L is verplicht het data-lek te melden bij de Autoriteit Persoonsgegevens. Zij doet dit binnen 72 uur nadat het data-lek bekend is. De melding omvat:

- Aard van de inbreuk;
- Maatregelen die genomen gaan worden of reeds zijn genomen;
- Een indicatie van de vermoedelijke gevolgen;
- Contactpersoon bij GIPS S&L.

Daarnaast zullen de betrokkenen waarop het data-lek van invloed is, geïnformeerd worden als dit een negatief effect heeft op de persoonlijke levenssfeer.

Afhankelijk van de aard en ernst van de datalekken en/of het misbruik kunnen de volgende maatregelen genomen worden: waarschuwing, ontzegging toegang tot gegevens, beëindiging van functie of taak, uitschrijven als medewerker, ontslag. Daarnaast zal onderzocht worden of er maatregelen ter voorkoming genomen kunnen worden. We spreken van misbruik wanneer:

- Een persoon die daartoe niet gerechtigd is gegevens verkrijgt en gaat gebruiken.
- Een in principe gerechtigd persoon de gegevens gebruikt voor een ander doel dat (hem/haar) is toegestaan.
- Gegevens gebruikt worden die niet geregistreerd of gebruikt mogen worden.

Functionaris gegevensbescherming en borging

Binnen GIPS is een medewerker benoemd als Functionaris Gegevensbescherming (FG). Deze taak staat in FM bij de opmerkingen van de betreffende medewerker. De FG beoordeelt één keer per jaar de werking van het privacy-beleid en de borging. De bevindingen rapporteert de FG aan de directie en het bestuur.

Privacy statement

Het privacy statement maakt deel uit van dit beleid. Het privacy statement is gepubliceerd op de website van GIPS S&L. Een exemplaar is ook opvraagbaar via de administratie van GIPS S&L.

Vragen en klachten

Voor vragen en/of klachten over registratie van persoonsgegevens kan contact opgenomen worden met de administratie van GIPS S&L.

Contactgegevens

GIPS S&L
Sint Pieterstraat 3
6463 CP Kerkrade

Tel.: 045-5312058
Mail.: info@gips-sl.nl
Website: www.gips-sl.nl