prime Visit en GDPR

1. GDPR / AVG

De Europe Unie heeft op 27 april 2016 de definitieve versie gepubliceerd van een wetgeving die er in de eerste plaats gekomen is voor de bescherming van privégegevens: de zogenaamde General Data Protection Regulation (GDPR), ook wel Algemene Verordening Gegevensbescherming (AVG) genoemd. Onder privégegevens verstaan we alle data die kan gelinkt worden aan een individu, zoals bijvoorbeeld bankkaartgevens, paswoorden, financiële gegevens, medische en sociale gegevens..enz. Met deze nieuwe wetgeving wil de EU in de eerste plaats de burgers terug meer controle geven over hun persoonlijke data. Een tweede belangrijk doel is de verdere ondersteuning van de digitale economie

De principes zijn grosso modo de volgende:

- **transparantie**: de persoon van wie de gegevens verwerkt worden, is hier van op de hoogte, heeft hiervoor toelating gegeven en kent zijn rechten
- **doelbeperking**: de persoonsgegevens worden voor een welbepaald gewettigd doel verzameld, en mogen niet voor andere zaken gebruikt worden
- **gegevensbeperking**: enkel de noodzakelijke gegevens die voor het beoogde doel noodzakelijk zijn, mogen worden verzameld
- **juistheid**: de persoonsgegevens moeten correct zijn en blijven
- **bewaarbeperking**: de persoonsgegevens mogen niet langer bewaard worden dan nodig voor het beoogde doel
- **integriteit en vertrouwelijkheid**: de persoonsgegevens moeten beschermd worden tegen toegang door onbevoegden, verlies of vernietiging
- **verantwoording**: de verantwoordelijke moet kunnen aantonen aan deze regels te voldoen

2. GDPR en prime Visit

We bekijken in dit document welke persoonlijke informatie er in prime Visit omgaat, om welke redenen die informatie aanwezig is en waarop de klant moet letten.

De applicatie prime Visit kent twee implementatiemodellen :

- Een on-premise installatie waarbij de klant zelf zorgt voor een server voor prime Visit en het beheer van die server.

- Als Software as a Service (SaaS), dus als cloud oplossing, waarbij GET de applicatie voor de klant in een datacenter beheert en de klant via een abonnementsformule toegang krijgt.

Het is duidelijk dat beide modellen in het kader van privacy tot verschillende verantwoordelijkheden leiden. We refereren daarom verder in dit document waar nodig naar de modelkeuze.

3. Persoonlijke informatie

We beginnen met een overzicht van de persoonlijke informatie die wordt opgeslagen in de database van prime Visit.

We onderscheiden 3 soorten gebruikers om de verschillen duidelijk te maken :

- Contactpersonen (gastheer, host, …)
- Bezoeker (dagbezoeker, contractor, transporteur, …)
- Gebruiker (receptionist, bewaking ,…)

3.1. Opgeslagen data voor Contactpersonen (gastheer, host)

Informatie	**Doel, gebruik**
Familienaam, 2de Naam en voornaam	Basisinformatie van de contactpersoon, als (onderdeel van een) unieke identificatie in het systeem
E-mailadres	Gebruikt voor het sturen van interne statuswijzigingen.
Vast telefoonnummer	Nodig zodat de bezoeker en/of gebruiker de contactpersoon kan bellen om (verder) af te spreken
Mobiel telefoonnummer	Nuttig zodat de bezoeker en/of gebruiker de contactpersoon kan bellen om (verder) af te spreken
Document(en)	Document(en) die nodig/nuttig zouden kunnen zijn bij een bepaalde bezoekersprocedure
Foto van de contactpersoon	Niet verplicht, kan eventueel gebruikt worden voor snelle identificatie van de contactpersoon door bezoeker en/of gebruiker.

Commentaar	Commentaar die nodig/nuttig zou kunnen zijn bij een bepaalde bezoekersprocedure
Afdeling	Informatie ter ondersteuning voor de bezoekers en/of gebruikers zodat ze hun contactpersoon snel kunnen opzoeken/vinden.
Locatie	Site, gebouw, kamer informatie nodig zodat de bezoeker en/of gebruiker de plaats van de vergadering kan vinden
Aanwezig?	Informatie ter ondersteuning voor de bezoekers en/of gebruikers zodat ze weten of de contactpersoon momenteel aanwezig is op de site
Gebruikersnaam	Nodig voor persoonlijke login van de medewerker. Niet van toepassing indien de klant werkt met optie single sign-on of Windows Authenticatie.
Wachtwoord	Nodig voor persoonlijke login van de medewerker. Niet van toepassing indien de klant werkt met optie single sign-on of Windows Authenticatie.

3.2. Opgeslagen data voor bezoekers

Informatie	**Doel, gebruik**
Familienaam, 2de Naam en voornaam	Basisinformatie van de bezoeker, als (onderdeel van een) unieke identificatie in het systeem
E-mailadres	Gebruikt voor het sturen van externe verwittigingen
Vast telefoonnummer	Nodig zodat men de bezoeker kan bellen om (verder) af te spreken
Mobile telefoonnummer	Nodig zodat men de bezoeker kan bellen om (verder) af te spreken
Bedrijfsnaam en locatie	Gebruikt voor dataconsistentie
Document(en)	Document(en) die nodig/nuttig zouden kunnen zijn bij een bepaalde bezoekersprocedure

Foto van de contactpersoon	Niet verplicht, kan eventueel gebruikt worden voor snelle identificatie van de bezoeker door de contactpersoon en/of gebruiker.
Commentaar	Commentaar die nodig/nuttig zou kunnen zijn bij een bepaalde bezoekersprocedure
Aanwezig?	Informatie ter ondersteuning voor de contactpersonen en/of gebruikers zodat ze weten of hun bezoeker momenteel aanwezig is op de site
Vrije velden	De klant kan zelf velden toevoegen aan de bezoekersdatabase. We zien volgende toepassingen: ▪ Gebruik in toegangsregels om toegang te geven of niet ▪ Persoonlijke informatie die nuttig is om te tonen aan een contactpersoon dat de bezoeker over de juiste informatie beschikt om een bezoek procedure af te mogen/kunnen handelen De klant kan in principe eender welke informatie kwijt in de vrije velden, zoals leeftijd, nummerplaat, ID kaart nummers, certificaties, wensen bij het bezoek…enz. Alhoewel deze data goed kan worden afgeschermd voor andere gebruikers dient te worden opgemerkt dat het bijhouden van zulke informatie in het kader van GDPR altijd een duidelijk doel moet hebben.
Paspoort/ID document scan	Een scan die kan gebruikt worden om eventueel de foto van de bezoeker te extraheren en/of de aanwezige MRZ informatie te interpreteren
Handtekening	Niet verplicht, kan eventueel gebruikt worden om rapporten of andere documenten samen te stellen die laten zien dat e bepaalde voorwaarden/regels/voorschriften ondertekend werden.

3.3. Opgeslagen data voor gebruikers

Informatie	**Doel, gebruik**
Familienaam, 2de Naam en voornaam	Basisinformatie van de bezoeker, als (onderdeel van een) unieke identificatie in het systeem
E-mailadres	Gebruikt voor het sturen van updates
Rol	Nodig zodat de juiste gebruiker binnen de juiste procedures kan werken

Veiligheidsgroep	Nodig zodat de juiste gebruiker alleen met de toegekende data kan werken
Contactpersoon	Niet verplicht, kan eventueel gebruikt worden voor snelle invoer van bezoeken voor een bepaalde de contactpersoon

4. Toegang tot de gegevens

4.1. Toegang in de prime Visit omgeving

De eindgebruiker werkt in prime Visit via zijn browser of een lokale Java client. De communicatie tussen de browser of client en de prime Visit server verloopt standaard niet versleuteld (HTTP) maar kan optioneel wel versleuteld worden. De klant dient hiervoor dan het nodige SSL certificaat te voorzien.

SaaS: bij klanten met de cloud oplossing verloopt de communicatie altijd via HTTPS en is de cloud server in principe vanop het hele internet toegankelijk; een goede keuze van gebruikersnaam en wachtwoord is in deze dus extra belangrijk.

4.2. Rollen en login

In prime Visit kan men voor elke gebruiker één of meer rollen definiëren. In een rol wordt bepaald welke gegevens de medewerker mag raadplegen over zichzelf en bezoekers en contactpersonen. Typische rollen zijn: receptionist, bewaker, sysadmin, …enz.

De toegang verloopt steeds met gebruikersnaam en wachtwoord (eventueel via single sign-on).

- **Receptionisten** hebben typisch enkel toegang tot hun eigen gegevens en die van hun toegewezen contactpersoon en de bezoekers
- **Bewakers** hebben typisch toegang tot gegevens van alle contactpersonen en bezoekers zoals aan- en afwezigheden.
- **Sysadmins** hebben typisch toegang tot alle gegevens, al kan er hier ook voor gezorgd worden dat ze meer of minder info te zien krijgen.

4.3. Authenticatie

De applicatie beschikt over volgende keuzes wat betreft authenticatie van de gebruikers:

- Gebruikersnaam en wachtwoord worden beheerd in de applicatie. Het wachtwoord van de medewerker wordt versleuteld in de database opgeslagen en kan niet in omgekeerde richting weer leesbaar worden gemaakt.

Op het moment van schrijven dient een wachtwoord in prime Visit enkel te voldoen aan een instelbare minimumlengte. Men kan het systeem zelf een wachtwoord laten genereren indien gewenst. Dit zal later worden uitgebreid met allerlei gebruikelijke strengere regels.

- LDAP en Windows Domein authenticatie: gebruikersnamen worden wel beheerd in prime Visit, wachtwoorden niet: wanneer de medewerker zijn wachtwoord invult, wordt dat doorgestuurd naar de domein server van het bedrijf die beslist over de authenticatie.

- Single sign-on via Windows Domain.

4.4. Server

prime Visit wordt steeds op een server met Windows Server operating system geïnstalleerd: de applicatie bestaat uit een database systeem (zie verder), een webserver en enkele verwerkingsprocessen.

Gebruikers of contactpersonen of bezoekers behoeven geen rechtstreekse toegang tot de server, zij hebben voldoende aan de Java client of de web interface of de kiosk of de Outlook Plug-in. In principe heeft alleen een IT-beheerder toegang nodig tot de server en eventuele supportmedewerkers van GET.

Omwille van export- en importmogelijkheden (zie verder) kunnen (leesbare) Excel en/of PDF bestanden op de server circuleren. Het is dus belangrijk de toegang tot de server en de gedeelde mappen op de server strikt te regelen.

4.5. Database

Voor het databasesysteem waarin alle informatie wordt opgeslagen kan de IT beheerder kiezen tussen IBM DB2, My SQL, MS SQL, Maria DB, Oracle DB. De database bevindt zich in bijna alle gevallen op de prime Visit server zelf. De data in de database is niet versleuteld. De database is alleen toegankelijk met gebruikersnamen en wachtwoorden van apart aangemaakte Windows gebruikers, die voor geen enkele andere toepassing gebruikt worden.

Een IT-beheerder die toegang heeft tot de prime Visit server en ook de gebruikersnamen en paswoorden van de database gebruikers kent, kan zich m.a.w. volledige toegang verschaffen tot de data in de database.

4.6. Identiteitsscan

Optioneel kan de klant in prime Visit beschikken over een mogelijkheid om de gegevens van bezoekers via hun identiteitskaart of paspoort rechtstreeks in te lezen in de database (inclusief foto), bedoeld als comfort en om typfouten te vermijden:

- De klant bepaalt precies welke gegevens zullen worden bewaard in de database.
- Het uitlezen van de gegevens van de identiteitskaart gebeurt via de beschikbare MRZ gegevens op de daarvoor toegankelijke strook (zie onderkant van volgende foto als voorbeeld) :

5. Aan- en afwezigheden beschikbaar voor iedereen

Bij een koppeling aan een toegangscontrolesysteem kunnen, in prime Visit, aan- of afwezigheid van een contactpersoon en bezoeker wordt getoond aan gebruikers, via de client interface (Java of HTML).

6. Logging

Alle wijzigingen die gebruikers in de applicatie doen worden gelogd :

- Input en verwijderen van gegevens
- Aanpassingen in de configuratie
- Inlog pogingen

Bij elke wijziging wordt de ID van de gebruiker, tijdstip, ip-adres en info over de wijziging gelogd (wie, wat, waar, wanneer). Alle logging wordt bewaard in de database en is alleen raadpleegbaar door aangeduide personen.

7. Dataretentie en archivering

Standaard wordt alle data onbeperkt in de tijd bijgehouden. We raden wel aan om een maximale termijn worden in te stellen, ook omwille van performantieredenen. Zo kan men oudere gegevens automatisch uit de database laten halen en laten stockeren in archiefbestanden.

On-premise: de klant bepaalt of en waar archiverings bestanden terecht komen, hij is verantwoordelijk voor toegangsautorisaties tot de bestanden.

SaaS: GET is verantwoordelijk voor de archivatie, de bestanden blijven op de cloudserver bewaard. Op vraag kunnen zij over een beveiligde verbinding worden doorgestuurd.

8. Database back-ups

Standaard worden geen automatisch back-ups van de database genomen. De klant kan zelf een mechanisme instellen om via de database rechtstreeks back-up te nemen. Het prime Visit systeem heeft daar zelf geen tools voor voorzien.

On-premise: de klant bepaalt waar de back-up bestanden terecht moeten komen, hij is verantwoordelijk voor toegangsautorisaties tot de bestanden.

SaaS: GET is verantwoordelijk voor de back-ups, de bestanden blijven op de cloudserver bewaard en zijn dus alleen toegankelijk door personen die rechtstreeks toegang hebben tot de server.

9. Data in- en uit de applicatie

9.1. Rapporten en exports

Gebruikers van prime Visit kunnen toegang krijgen tot rapporten en exports met eventuele persoonlijke gegevens. Rapporten en exports kunnen vanuit de client en de webinterface worden gedownload en kunnen dus door de gebruiker op de lokale PC worden bewaard (Excel of PDF).

9.2. Import

Sommige gegevens kunnen vanuit andere systemen worden geïmporteerd. Dat is veelal het geval voor bulk import van bezoekers en/of bezoeken. De data dienen in dat geval als tekstbestand te worden aangeleverd aan de prime Visit server, waarna ze geïmporteerd worden. Optioneel kan het gegevensbestand na een succesvolle import automatisch worden verwijderd.

9.3. Koppeling met Outlook Exchange

Optioneel kunnen bezoeken ook ingegeven worden via een Outlook Plug in. Dit gebeurt over een beveiligde verbinding tussen de Outlook plug-in, prime Visit en de Exchange server.

9.4. Database views

De klant kan optioneel toegang krijgen tot de database via database views. Hiervoor wordt een aparte toegang met gebruikersnaam en wachtwoord ingesteld. Daarmee heeft hij geen toegang tot de volledige database, maar wel tot de meest gebruikte persoonsgegevens, en dit steeds van alle personen.

10. Back-up gebruikers

Een teamleader of andere verantwoordelijke kan in prime Visit een collega (back-up) aanduiden om zijn taken in prime Visit over te nemen wanneer hij afwezig is:

- Als de back-up gebruiker toegang heeft, dan erft hij alle rechten van de originele gebruiker over. Eventueel kan wel worden verhinderd dat hij acties op zichzelf kan doorvoeren (vaak is een back-up gebruiker immers een ondergeschikte).
- De verantwoordelijke geeft zelf aan vanaf wanneer, tot wanneer de back-up gebruiker toegang heeft.
- Alle acties die de back-up gebruiker doet worden gelogd onder zijn naam.
- De personeelsverantwoordelijke bepaalt op voorhand wie de gebruiker mag aanduiden als back-up gebruikers.

11. Disclaimer

Er is een mogelijkheid om in de kiosk interface van prime Visit een korte disclaimer te plaatsen voor bezoekers.

12. Recht om gegevens te bekijken

Contactpersonen, bezoekers en gebruikers hebben het recht om de gegevens die u bewaart in het systeem in te kijken en ook te wijzigen indien gewenst. Daar kan u aan tegemoet komen door persoonlijke gegevens die in de database bewaart te laten corrigeren door de gebruikers (typisch receptionisten of bewakers).

13. Tekst voorspellend vermogen, data consistentie

Het is mogelijk om het systeem te laten voorspellen wat u zou willen ingeven door de database dynamisch en content specifiek te doorzoeken op matches en die voor te stellen. Dit zal ook leiden tot betere dataconsistentie. Het is echter mogelijk dat deze tekst voorspellende functie misbruikt kan worden om de database te “onderzoeken” . De tekst voorspellende functie is echter optioneel en kan desgewenst afgezet worden.

14. Security updates

On-premise: de klant is verantwoordelijk voor het up-to-date houden van het operating system van de server, met de nodige security updates. Als de klant een onderhoudscontract heeft, dan is GET verantwoordelijk voor het up-to-date houden van de prime Visit software, inclusief security updates van het database systeem.

SaaS: GET is verantwoordelijk voor het up-to-date houden van de hele server, hiervoor zijn de nodige automatische waarschuwingssystemen voor ingesteld.