prime Time 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 Time

We bekijken in dit document welke persoonlijke informatie er in prime Time en de verwante opties prime Cost en prime Plan omgaat, om welke redenen die informatie aanwezig is en waarop u als klant moet letten.

De applicatie prime Time kent twee implementatiemodellen:

- Een **on-premise** installatie waarbij de klant zelf zorgt voor een server voor prime Time 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 Time, prime Plan en prime Cost:

Informatie	**Doel, gebruik**
Naam en voornaam	Basisinformatie van de medewerker
Taal	Nodig voor aanbieden van informatie in de juiste taal
Personeelsnummer	Nodig voor unieke identificatie van de medewerker. Opgelet: sommige klanten vullen hier het rijksregisternummer van de medewerker in. Dit raden we af, omdat personeelsnummers in allerlei schermen en rapporten te zien zijn, soms ook voor collega's en leidinggevenden.
E-mail adres	Gebruikt voor het sturen van statuswijzigingen over aanvragen, maar niet verplicht.
Nummer van de badge	Nodig voor identificatie van de medewerker aan de badgelezer
In dienst, uit dienstdatum	Nodig voor correcte verwerking van de tijdregistratie.
Foto van de medewerker	Niet verplicht, gebruikt voor makkelijke identificatie van de medewerker door de personeelsverantwoordelijken, maar ook in voor iedereen toegankelijke schermen zoals aan- en afwezigheden en dashboard (zie verder).
Afdeling	Gebruikt voor indelen van medewerkers in schermen en rapporten.
Gebruikersnaam	Nodig voor persoonlijke login van de medewerker.
Wachtwoord	Nodig voor persoonlijke login van de medewerker. Niet van toepassing indien de klant werkt met optie single sign-on of Windows Authenticatie.
Werkplan, persoonlijke vrije dagen en andere velden	Nodig voor correcte verwerking van de tijdregistratie.

gerelateerd aan tijdregistratie	
Vrije velden	De klant kan zelf velden toevoegen aan de personeelsdatabase. We zien volgende toepassingen: Gebruik in rekenregels voor verwerking van tijdregistratie: bv. geboortedatum voor aantal jaren dienst, aantal kilometers woon-werkverkeer, vakantierechten….etc.) Persoonlijke informatie die nuttig is om te tonen aan bv. teamleader of personeelsverantwoordelijken in het kader van de applicatie zoals telefoonnummer om de medewerker te kunnen bereiken als zijn planning wijzigt, De klant kan in principe eender welke informatie kwijt in de vrije velden, zoals adres, contractinformatie, telefoonnr., nummerplaat, info over kinderen…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.
Afwezigheden	Alle mogelijke afwezigheden zoals vakantie, ziekte, ADV, klein verlet…enz. worden opgeslagen in het systeem onder afwezigheidscodes. Die worden gebruikt voor een correcte tijdregistratie, maar ook voor het weergeven van de aan- of afwezigheid van een medewerker aan zijn collega's (zie verder). Afwezigheden worden ook geteld in tellers zoals opgenomen vakantie, glijsaldo, aantal dagen ziekte…enz.
Vakantierechten	Aantal dagen vakantie en andere soorten afwezigheden waarop de medewerker recht heeft. Indien de klant een optie voor automatische rechtenberekening heeft, dan heeft die module gegevens zoals geboortedatum en tewerkstellingspercentage nodig.
Geregistreerde en berekende zaken zoals prestaties, overuren, premies, maaltijdvergoeding, dienstreis, wachtdienst, fietsvergoeding…etc.	Nodig voor correcte tijdregistratie.
Afwijkingen zoals 'niet geboekt', 'te weinig dagprestatie', 'te lange lunchpauze', 'ongewettigd afwezig'…enz.	Nodig voor signaleren van mogelijke problemen aan specifieke gebruikers. Niet verplicht.
Roosterinformatie	Nodig voor correcte planning en tijdregistratie.
Ziektebriefjes	Optioneel kan de medewerker zijn afwezigheid verantwoorden d.m.v. een ziektebriefje als bijlage bij een afwezigheidscode: dit

	wordt dan bewaard in de database zodat de personeelsverantwoordelijke het kan bekijken en controleren. Dit soort van bijlagen kan steeds goed afgeschermd worden voor onbevoegde collega's.
Kwalificaties	In de optie prime Plan kan de klant informatie rond kwalificaties van de medewerker bijhouden zodat het planningssysteem hiermee rekening kan houden bij het plannen op bepaalde werkplekken waarvoor de medewerker gekwalificeerd moet zijn. De planner heeft dan normaal gezien een zicht op alle kwalificaties van de medewerkers die hij beheert.
Timesheet en jobtijdregistratie	In de optie prime Cost kan de medewerker een timesheet invullen met informatie over de projecten en activiteiten die hij uitgevoerd heeft, of op een kiosk-PC aangeven met welk order, project, activiteit…enz. hij gaat starten.

4. Toegang tot de gegevens

Wie heeft toegang tot de gegevens, en op welke manier? Hoe wordt de toegang beveiligd? We lichten de verschillende aspecten toe:

4.1. Toegang in de prime Time omgeving

De eindgebruiker werkt in prime Time via zijn browser. De communicatie tussen de browser en prime Time 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 Time kan men voor elke medewerker één of meer rollen definiëren. In een rol wordt bepaald welke gegevens de medewerker mag raadplegen over zichzelf en andere medewerkers. Typische rollen zijn: medewerker, teamleader, centraal beheerder, receptionist…enz.
De toegang verloopt steeds met gebruikersnaam en wachtwoord (eventueel via single sign-on).

> **Medewerkers** hebben typisch enkel toegang tot hun eigen gegevens en eventueel aan- en afwezigheidsinformatie (zonder verdere details) van hun collega's, bv. in een teamplanning.

Teamleaders hebben typisch toegang tot gegevens van hun medewerkers zoals aan- en afwezigheden, prestaties en planning. De beheerder bepaalt welke persoonlijke gegevens de teamleader mag zien.

Personeelsverantwoordelijken hebben typisch toegang tot alle gegevens, al kan er hier ook voor gezorgd worden dat bepaalde verantwoordelijken 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 Time enkel te voldoen aan een instelbare minimumlengte. Dit wordt in de loop van het voorjaar van 2018 uitgebreid met allerlei gebruikelijke strengere regels.

- LDAP en Windows Domein authenticatie: gebruikersnamen worden wel beheerd in prime Time, 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 of SAML.

4.4. Server

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

Eindgebruikers behoeven geen rechtstreekse toegang tot de server, zij hebben voldoende aan de web interface. 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 talloze (leesbare) tekstbestanden 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

Het databasesysteem waarin alle informatie wordt opgeslagen is IBM DB2. Het bevindt zich in bijna alle gevallen op de prime Time 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 Time 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. Mobile

prime Mobile is een optie binnen prime Time voor de medewerker en de teamleader, bedoeld voor smartphone en tablet. prime Mobile is een zogenaamde 'web app': de gebruiker installeert m.a.w. niets op zijn toestel maar surft met de browser van het toestel naar de prime Time web-server. Login verloopt steeds met gebruikersnaam en wachtwoord. Versleutelde HTTPS-communicatie is vereist.

De gebruiker van prime Mobile heeft toegang tot een subset van de gegevens die hij in de gewone web interface ziet.

Optioneel kan de locatie van de medewerker worden doorgegeven bij in- of uitboeken. De medewerker moet hiervoor steeds zijn toestemming geven. Iedereen die de boeking mag bekijken in prime Time, kan dan ook de locatie raadplegen.

4.7. E-ID

Optioneel kan de Belgische klant in prime Time beschikken over een mogelijkheid om de gegevens van de identiteitskaart van een medewerker 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 standaard beschikbare software van de Federale Overheid.

5. Aan- en afwezigheden beschikbaar voor iedereen

Er zijn enkele optionele toepassingen in prime Time en prime Plan waarin de aan- of afwezigheid van een medewerker wordt getoond aan collega's, via een web interface en zonder persoonlijke login: iedereen in het bedrijf kan die informatie dus zien. In alle gevallen is gevoelige informatie zoals het de specifieke soort afwezigheid (bv. bij ziekte) wel afgeschermd.

- Optie **Aan- en afwezighedenoverzicht**: men heeft hierin een overzicht van aan- of afwezigheid van alle collega's of een deel daarvan op het huidig moment, voor huidige week en komende weken.
  De klant kan in deze toepassing ook contactinformatie zoals foto, telefoonnummer en e-

mail adres ter beschikking stellen.

- Optie **Aan- en afwezigheden dashboard**: is een variant van Aan- en afwezigheidsoverzicht en geeft een compact overzicht van de aan- en afwezigheid van collega's op het huidig moment. Dit overzicht is bedoeld voor display op schermen in bv. inkomhal of receptie zodat snel duidelijk is wie aanwezig is.
  Het is aangeraden om deze informatie niet te tonen op plaatsen waar ook niet personeelsleden zoals bezoekers toegang hebben.

- **prime Plan dashboard**: biedt een overzicht aan medewerkers over de werkplek waarop zij moeten werken en de planning van de komende dagen. Vaak getoond op displays in bv. inkomhal.
  Het is aangeraden om deze informatie niet te tonen op plaatsen waar ook niet personeelsleden zoals bezoekers toegang hebben.

De toegang tot deze toepassingen wordt vanaf versie 2.2.03 van prime Time (feb. 2018) standaard alleen toegestaan intern vanop het bedrijfsnetwerk. Wil u bepaalde medewerkers ook toegang geven buiten het bedrijfsnetwerk, dan kan dat op IP-adres of -range worden ingesteld.

6. Logging

Vele wijzigingen die gebruikers in de applicatie doen worden gelogd :

- alle personeelsgegevens.
- ingave van aan- en afwezigheden, prestaties, goedkeuringen van overuren…enz.
- inloggegevens

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 in te stellen, ook omwille van performantieredenen. Zo kan men oudere gegevens automatisch uit de database laten halen en laten stockeren in archiefbestanden. Archiefbestanden zijn eenvoudige, leesbare tekstbestanden.

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

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

Ook de gegevens van medewerkers die uit dienst zijn blijven bewaard in de database, en dat is vaak ook wettelijk verplicht. Als de gegevens niet meer nodig zijn kan de klant de medewerker manueel verwijderen uit de database: alle informatie inclusief boekingen, aan- en afwezigheden, prestaties e.d. worden dan onherroepelijk mee verwijderd.

8. Database back-ups

Standaard worden dagelijks automatisch back-ups van de database genomen, en dit voor de laatste 3 dagen. Het aantal dagen is instelbaar. Een database back-up resulteert in een aantal bestanden.

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

Een tijdregistratie- en aan- en afwezighedensysteem bevat typisch enkele tools om data te importeren en te exporteren of te rapporteren. U transporteert m.a.w. gegevens vanuit een ander systeem naar prime Time, en omgekeerd. We bekijken enkele aandachtspunten:

9.1. Rapporten en exports

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

9.2. Loonkoppelingen

prime Time heeft specifieke koppelingen met tal van loonsecretariaten en interimkantoren voor het doorgeven van prestaties, afwezigheden, overuren e.d. uit prime Time. Dit zijn allemaal opties, alleen de aangekochte opties zullen actief zijn bij de klant. In de meeste gevallen verloopt de koppeling als volgt:

- De personeelsbeheerder start een export voor bepaalde medewerkers, voor een bepaalde periode.

- Het resultaat is een tekstbestand (ASCII of XML) dat voldoet aan het formaat dat afgesproken is met het loonsecretariaat of interimkantoor. Dat bestand wordt gedownload naar de lokale PC van de personeelsverantwoordelijke.
  Als alternatief kan de personeelsverantwoordelijke ervoor kiezen om het exportbestand niet te downloaden maar op de server te laten staan en van daar verder te transporteren.

- De personeelsverantwoordelijke importeert het bestand in het externe pakket of stuurt het bv. via e-mail op naar het loonsecretariaat. Hij is zelf verantwoordelijk voor het verwijderen van het bestand op zijn PC.

In enkele gevallen verloopt de communicatie van de gegevens rechtstreeks tussen prime Time en een server van het loonsecretariaat (machine to machine) over een beveiligde verbinding. Meestal heeft de personeelsverantwoordelijk in zo'n geval ook de mogelijkheid tot inzage van wat er doorgestuurd wordt.

9.3. Import

Sommige gegevens kunnen vanuit andere systemen worden geïmporteerd. Dat is veelal het geval voor personeelsgegevens omdat die meestal al in een andere applicatie aanwezig zijn. De data dienen in dat geval als tekstbestand te worden aangeleverd aan de prime Time server, waarna ze geïmporteerd worden. Optioneel kan het gegevensbestand na een succesvolle import automatisch worden verwijderd.

9.4. Koppeling met Outlook Exchange

Optioneel kunnen afwezigheden van medewerkers ook doorgestuurd worden naar hun Outlook kalender. Dit gebeurt over een beveiligde verbinding tussen prime Time en de Exchange server.

9.5. 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 Time een collega (back-up) aanduiden om zijn taken in prime Time 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 webinterface van prime Time op de home page, en op alle PDF rapporten een korte disclaimer te plaatsen (tekst op één lijn).

12. Recht om gegevens te bekijken

Uw medewerkers hebben het recht om de gegevens die u bewaart in het systeem in te kijken en ook te wijzigen. Daar kan u aan tegemoet komen door de gegevens die u in het personeels-scherm invoert ook aan de medewerker ter beschikking te stellen in zijn toegang tot prime Time. Onze supportmedewerkers kunnen u daarbij helpen. U kan voor elk gegeven instellen of u dit 'al-leen lezen' wil tonen (in dat geval moet de medewerker de personeelsdienst contacteren als hij iets gewijzigd wil zien) of ook wijzigbaar wil maken.

13. Security updates van besturingssysteem

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 Time software, inclusief secu-rity 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.

14. Badgelezernetwerk

Via badgelezers kunnen medewerkers in- en uitboeken op het bedrijf en kunnen zij bepaalde per-soonlijke informatie zoals de laatste boekingen en een maand of vakantiesaldo raadplegen op de terminal (instelbaar). De medewerker dient zich hierbij kenbaar te maken met zijn badge.

Boekingen worden op de terminal bewaard en doorgestuurd naar de server over het standaard TCP/IP netwerk van de klant. De server downloadt op regelmatige tijdstippen informatie over de laatste boekingen en maand- of vakantiesaldo naar de badgelezer zodat die informatie onmiddel-lijk kan worden getoond wanneer de medewerker een volgende keer boekt. De gegevens blijven in principe onbeperkt in de badgelezer bewaard. Gegevens van medewerkers die uit dienst zijn worden automatisch gewist.

De communicatie tussen de badgelezer en het netwerk verloopt via een bedrijfseigen protocol en is op het moment van schrijven niet versleuteld.

- Voor de DT1000 zal dit in de loop van 2018 gewijzigd worden naar een versleutelde verbinding (in te stellen). Ook wordt de toegang tot de badgelezer via het netwerk strenger beveiligd.
- Voor de DT100 en Falcon zijn er geen plannen voor versleuteling.
- Het toekomstige gamma van badgelezers, de ADT familie, zal standaard versleutelde communicatie bieden.

SaaS: als de klant een netwerk van badgelezers heeft, dan zullen de badgelezers met de cloud server worden verbonden via een beveiligde verbinding (VPN).

14.1. Badges en koppeling met ID Works

Op de badge van een medewerker wordt alleen een uniek badgenummer gestockeerd.

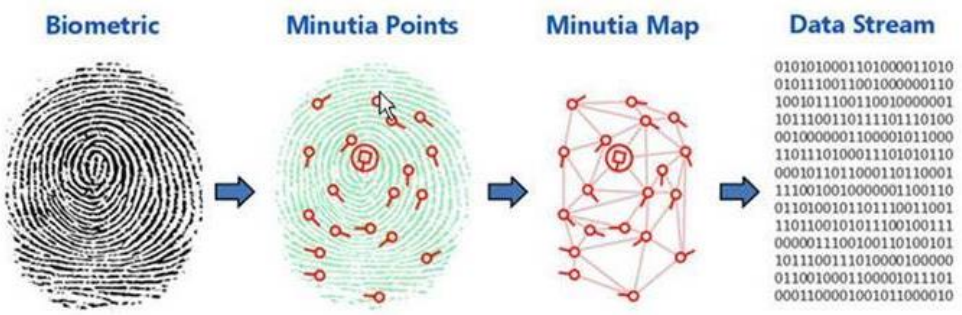
Badges kunnen ook bedrukt worden, door GET of door de klant zelf. Welke gegevens er dan op de badge moeten voorkomen kan volledig bepaald worden.

Voor klanten die zelf badges willen bedrukken is er het extern pakket ID Works ter beschikking, dat een koppeling legt met de database van prime Time, maar enkel toegang krijgt tot enkele basisgegevens zoals naam, afdeling, badgenummer, foto. Het pakket kan mogelijk de foto's van medewerkers opslaan op de PC waarop het geïnstalleerd is.

14.2. Biometrische gegevens

Badgelezers met de zogenaamde 'fingerprint' optie hebben als voordeel dat men geen badges moet uitreiken, en dat men meer zekerheid heeft over de identiteit van degene die op de badgelezer boekt. De werking is als volgt:

- Eenmalig vraagt de personeelsverantwoordelijke aan de medewerker om één of meer vingerafdrukken te registreren in het systeem via een toestel op de personeelsdienst (enrollment). Een foto van elke vingerafdruk op zich wordt niet bewaard, wel een via een wiskundig algoritme berekende 'template'. Het proces om van de vingerafdruk tot een template te komen is een ‘one-way’ proces, iemand die de template in handen krijgt kan dus niet omgekeerd de volledige vingerafdruk bekomen.



De templates (data stream) worden bewaard in de database, via een beveiligde verbinding.

- De templates worden gedownload naar alle badgelezers in het bedrijf die voorzien zijn van een vingerafdruksensor, zodat die de medewerkers snel kan identificeren.

- Wanneer de medewerker boekt met een vingerafdruk worden bij het doorsturen van de boeking naar de server geen gegevens over de vingerafdruk gebruikt.