Crossuite verwerkersovereenkomst

Partijen

Opdrachtgever, verder te noemen PRAKTIJK,

en:

CROSSUITE bv gevestigd op Uitbreidingstraat 390, 2600 Antwerpen, België
dezen rechtsgeldig vertegenwoordigd door Van den Putte Joris en Debreuck Nicolas verder *'CROSSUITE'* genoemd.

in aanmerking nemende dat:

A. PRAKTIJK een patiëntenbeheerplatform in de vorm van een webapplicatie (verder "Portaal"), ontwikkeld door CROSSUITE, in gebruik wenst te nemen.
B. PRAKTIJK en CROSSUITE hiertoe een Overeenkomst hebben gesloten
C. In het kader van die Overeenkomst verwerkt CROSSUITE Persoonsgegevens, verkregen door PRAKTIJK
D. In deze verwerkersovereenkomst zijn de afspraken die gemaakt zijn tussen PRAKTIJK en CROSSUITE over het verwerken van de Persoonsgegevens vastgelegd
E. In aanvulling op het bepaalde in de Overeenkomst, komen Partijen in het licht van GDPR en wbp (wet bescherming persoonlijk levensfeer) het volgende overeen.

Artikel 1. Definities

1.1 In deze Verwerkersovereenkomst hebben de volgende begrippen, steeds aangeduid met een hoofdletter, zowel in enkelvoud als in meervoud, de volgende betekenis:

a. Betrokkene: Degene op wie de Persoonsgegevens betrekking hebben, zoals bedoeld in Art 4(1) GDPR;
b. Bewerker: De bewerker als bedoeld in artikel 4(8) GDPR. In deze Verwerkersovereenkomst CROSSUITE;
c. Verwerkersovereenkomst: Deze Verwerkersovereenkomst, welke onlosmakelijk onderdeel uitmaakt van de Overeenkomst, ter neerlegging van de afspraken zoals bedoeld in de GDPR;
d. Overeenkomst: Het geheel van de tussen PRAKTIJK en CROSSUITE gesloten overeenkomsten/contracten inclusief bijlagen ten behoeve van ingebruikname van het Portaal;
e. Datalek: Verlies of ongeautoriseerde verwerking van Persoonsgegevens, of het bekend worden van een gebrek in de beveiliging die een aanmerkelijk risico daarop teweegbrengt;
f. Partijen: PRAKTIJK en CROSSUITE;
g. Persoonsgegevens: Gegevens die direct of indirect herleidbaar zijn tot een natuurlijk persoon, zoals bedoeld in artikel 4(1) GDPR;
h. Verantwoordelijke: De verantwoordelijke als bedoeld in artikel 4(7) GDPR. In deze Verwerkersovereenkomst is de verantwoordelijke de PRAKTIJK;
i. Verwerking: Elke handeling of elk geheel van handelingen met betrekking tot Persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van Persoonsgegevens, zoals bedoeld in art 4(2) van de GDPR.

Artikel 2. Duur en beëindiging

2.1 Deze Verwerkersovereenkomst eindigt van rechtswege op het moment dat de (licentie) Overeenkomst eindigt.
2.2 CROSSUITE zal bij beëindiging van de Overeenkomst op verzoek en naargelang de keuze van PRAKTIJK de Persoonsgegevens ofwel in een gangbaar formaat ter beschikking stellen aan de PRAKTIJK of aan een door PRAKTIJK aangewezen Derde, ofwel de Persoonsgegevens met inbegrip van alle bestaande kopieën ervan wissen. Na het voltooien van deze handeling(en), maakt CROSSUITE haar slotfactuur over aan de PRAKTIJK voor de nog af te rekenen prestaties.
2.3 CROSSUITE zal na overdracht van de Persoonsgegevens aan PRAKTIJK de nog aanwezige Persoonsgegevens die redelijkerwijze niet aan de andere partij ter hand kunnen worden gesteld, vernietigen. In dit geval zal CROSSUITE tevens zorgdragen voor vernietiging van de Persoonsgegevens bij de Sub-bewerkers.

Artikel 3. Reikwijdte van Verwerkersovereenkomst en Verwerking door CROSSUITE

3.1 CROSSUITE zal de Persoonsgegevens die ter beschikking worden gesteld enkel verwerken met het oog op de uitvoering van de Overeenkomst.

3.2 PRAKTIJK stelt de doeleinden vast voor de Verwerking van Persoonsgegevens. CROSSUITE verwerkt Persoonsgegevens in opdracht van PRAKTIJK uitsluitend met als doel het faciliteren van het Portaal.

3.3 PRAKTIJK stelt CROSSUITE op de hoogte van verwerkingsdoeleinden voor zover deze niet reeds in deze Verwerkersovereenkomst zijn genoemd. In bijlage 1 bij deze Verwerkersovereenkomst zijn de door PRAKTIJK gestelde verwerkingsdoeleinden geformuleerd en maken onverbrekelijk deel uit van deze Verwerkersovereenkomst. CROSSUITE zal de Persoonsgegevens niet voor een ander doeleinde Verwerken dan door PRAKTIJK is vastgesteld.

3.4 CROSSUITE Verwerkt de Persoonsgegevens uitsluitend binnen de Europese Unie.

Artikel 4. Beveiliging

4.1 CROSSUITE zal zorgen voor een adequaat niveau van beveiliging van de door haar Verwerkte Persoonsgegevens tegen misbruik en ongeauthoriseerd gebruik.

4.2 CROSSUITE neemt passende technische en organisatorische maatregelen om de Persoonsgegevens van PRAKTIJK te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. CROSSUITE draagt zorg voor de nodige technische en organisatorische aard m.b.t. tot de beveiliging volgens de norm NEN 7510, waarvoor Crossuite is gecertificeerd (TPM 2017). De datacenters waar CROSSUITE gebruik van maakt voldoen aan de ISO27001 norm.
Deze maatregelen worden aangemerkt als een passend beveiligingsniveau in de zin van art. 32 van de GDPR. PRAKTIJK is gerechtigd om in overleg met CROSSUITE tijdens de looptijd van de Overeenkomst door een onafhankelijke deskundige de naleving hiervan te controleren, bijvoorbeeld door middel van het uitvoeren van een audit. PRAKTIJK zal alle kosten in verband met deze controle dragen.

4.3 CROSSUITE verklaart in ieder geval de volgende maatregelen te hebben genomen:
- Logische toegangscontrole, 2-step authenticatie
- Fysieke maatregelen voor toegangsbeveiliging
- SSL verbindingen
- Registratie security incidenten
- Doelgebonden toegangsbeperkingen
- Controle op toegekende bevoegdheden.

CROSSUITE kan ieder moment de maatregelen eenzijdig aanpassen, maar alleen zonder het niveau van de beveiliging te verminderen.

4.4 PRAKTIJK is verantwoordelijk voor de naleving van de door Partijen genomen Maatregelen (zie Overeenkomst CROSSUITE).

4.5 CROSSUITE staat er niet voor in dat de beveiliging onder alle omstandigheden doeltreffend is. De beveiliging zal echter steeds voldoen aan een niveau dat, gelet op de stand van de techniek, de gevoeligheid van de Persoonsgegevens en de, aan het treffen van de beveiliging verbonden, kosten niet onredelijk zijn.

4.6 Op eerste verzoek van CROSSUITE zal PRAKTIJK binnen 2 werkdagen CROSSUITE schriftelijk informeren over de wijze waarop PRAKTIJK uitvoering geeft aan haar verplichtingen, op grond van de wet- en regelgeving, op het gebied van de bescherming van Persoonsgegevens, waaronder in ieder geval begrepen de Wbp en GDPR.

4.7 CROSSUITE staat de PRAKTIJK voor de verwerking bij in het nakomen van diens verplichtingen onder de GDPR. CROSSUITE verleent bijstand aan de PRAKTIJK voor de Verwerking in het kader van het uitvoeren van een gegevensbeschermingseffectbeoordeling overeenkomstig artikel 35 en 36 van de GDPR.

Artikel 5. Audits

5.1 PRAKTIJK heeft het recht om periodiek audits uit te (laten) voeren ter controle van de afspraken onder deze Verwerkersovereenkomst.

5.2 CROSSUITE zal de voor de audits benodigde ondersteunende gegevens zoals systeemlogs bewaren.

5.3 De personen die de audit uitvoeren zullen zich conformeren aan de beveiligingsprocedures zoals die bij CROSSUITE van kracht zijn.

5.4 CROSSUITE zal aan de audit meewerken en alle voor de audit redelijkerwijs relevante informatie zo tijdig mogelijk ter beschikking stellen.
5.5 De kosten van een audit worden door PRAKTIJK gedragen.
5.6 PRAKTIJK zal niet eerder aanvangen met een audit dan 14 (veertien) dagen na voorafgaande schriftelijke aankondiging. Indien datum en tijdstip van de audit CROSSUITE niet gelegen komt, zal CROSSUITE daarvan PRAKTIJK op de hoogte stellen en een voorstel doen voor een vervangende datum.

Artikel 6. Vrijwaringen

6.1 CROSSUITE vrijwaart PRAKTIJK tegen elke rechtsvordering van derden, uit welke hoofde dan ook, in verband met de Persoonsgegevens of de uitvoering van de Verwerkersovereenkomst en/of Overeenkomst, tenzij CROSSUITE bewijst dat zij conform de instructies van de PRAKTIJK heeft gehandeld, en/of alle technische en organisatorische maatregelen ter beveiliging van de Persoonsgegevens te hebben genomen zoals omschreven in deze Verwerkersovereenkomst.
6.2 PRAKTIJK vrijwaart CROSSUITE tegen elke rechtsvordering van derden, uit welke hoofde dan ook, in verband met de Persoonsgegevens of de uitvoering van de Verwerkersovereenkomst en/of Overeenkomst, indien vaststaat dat CROSSUITE louter conform de instructies van PRAKTIJK heeft gehandeld.
6.3 Zijn de rechtsvorderingen van derden in verband met de Persoonsgegevens of de uitvoering van de Verwerkersovereenkomst en/of Overeenkomst het gevolg van opzet of grove nalatigheid gepleegd door een partij dan is die partij in ieder geval vrijwaring verschuldigd ten aanzien van de andere partij.

Artikel 7. Geheimhouding

7.1 Op alle Persoonsgegevens die CROSSUITE van PRAKTIJK ontvangt en/of zelf verzamelt of dient te verzamelen met het doel deze te Verwerken overeenkomstig het in de Overeenkomst daartoe bepaalde, rust een geheimhoudingsplicht jegens derden.
7.2 CROSSUITE is zich bewust dat de informatie die de klant met CROSSUITE deelt en opslaat binnen het Portaal een geheim en bedrijfsgevoelig karakter heeft. Alle CROSSUITE medewerkers zullen gedurende hun dienstverband en daarna, zoals in hun arbeidsovereenkomst met geheimhoudingsclausule is opgenomen, op verantwoorde wijze met de informatie van PRAKTIJK omgaan.
7.3 CROSSUITE zal deze informatie niet voor een ander doel gebruiken dan waarvoor zij deze heeft verkregen, zelfs niet wanneer deze in een zodanige vorm is gebracht zodat deze niet tot PRAKTIJK of natuurlijke personen, zoals de Betrokkene, herleidbaar is.
7.4 De geheimhoudingsplicht is niet van toepassing voor zover PRAKTIJK of de Betrokkene zelf uitdrukkelijk toestemming heeft gegeven of indien en voor zover er een wettelijke verplichting bestaat om informatie aan een derde te verstrekken.
7.5 Indien CROSSUITE van de diensten van derden gebruik maakt, zorgt zij er onvoorwaardelijk voor dat deze derden dezelfde geheimhoudingsplicht als tussen Partijen is overeengekomen schriftelijk zal aanvaarden en deze geheimhoudingsplicht ook strikt zal naleven.
7.6 Medewerkers met toegang tot Persoonsgegevens van PRAKTIJK:
1. Systeembeheerders van CROSSUITE hebben volledige toegang tot de gegevens van de PRAKTIJK voor:
   - het plaatsen van een nieuwe versie, build of update;
   - het doorvoeren van patches en hotfixes;
   - het maken van een back-up;
   - het verplaatsen van een omgeving.
2. Consultants, supportmedewerkers en andere CROSSUITE medewerkers hebben toegang tot hetgeen waar zij toestemming voor hebben ontvangen van de PRAKTIJK en voor zolang zij toestemming hebben van de PRAKTIJK.

Artikel 8. Meldplicht

In geval van ontdekking van een Datalek zal CROSSUITE, de PRAKTIJK zo spoedig mogelijk en uiterlijk binnen de 24 uren na de ontdekking hierover informeren via 0032 2 888 91 79 of op volgend e-mailadres: info@crossuite.com.
In geen geval zal CROSSUITE zélf de betrokkenen informeren over dit Datalek, onverminderd de verplichting de gevolgen van dergelijke inbreuken en incidenten zo snel mogelijk ongedaan te maken dan wel te beperken.

CROSSUITE zal voorts, op het eerste verzoek van de verwerkingsverantwoordelijke, alle inlichtingen verschaffen die de PRAKTIJK noodzakelijk acht om het incident te kunnen beoordelen.

CROSSUITE verbindt zich ertoe om na de ontdekking van een Datalek, de PRAKTIJK op de hoogte te houden van maatregelen die werden genomen teneinde de omvang van het Datalek te beperken dan wel teneinde dit in de toekomst te vermijden.

CROSSUITE beschikt over een gedegen plan van aanpak betreffende de omgang met en afhandeling van Datalekken en zal de PRAKTIJK, op diens verzoek, inzage verschaffen in het plan. Verwerker stelt de verwerkingsverantwoordelijke op de hoogte van materiële wijzigingen in het plan van aanpak.

CROSSUITE zal het doen van meldingen aan de toezichthouder(s) overlaten aan de PRAKTIJK.

CROSSUITE zal alle noodzakelijke medewerking verlenen aan het zo nodig, op de kortst mogelijke termijn, verschaffen van aanvullende informatie aan de toezichthouder(s) en/of betrokkene(n). Daarbij verschaft CROSSUITE in ieder geval de informatie, zoals beschreven in bijlage 3, aan de Verwerkingsverantwoordelijke.

De Verwerker houdt een gedetailleerd logboek bij van alle (vermoedens van) Datalekken, evenals de maatregelen die in vervolg op dergelijke Datalekken zijn genomen waarin minimaal de informatie zoals bedoeld in bijlage 3 is opgenomen, en geeft daar op eerste verzoek van de PRAKTIJK inzage in.

Artikel 9. Rechten van Betrokkene

In geval de PRAKTIJK een aanvraag ontvangt van de betrokkene van wie Persoonsgegevens worden verwerkt, om zijn rechten uit te oefenen overeenkomstig de GDPR zoals bv. recht van verzet of recht van wissing van de Persoonsgegevens, geeft de PRAKTIJK deze opdracht onverwijld door aan CROSSUITE.

CROSSUITE verbindt zich ertoe om onverwijld en dit uiterlijk binnen 7 werkdagen na ontvangst van de aanvraag, een passend gevolg te geven aan deze opdracht van de PRAKTIJK en ofwel de gevraagde informatie te verschaffen ofwel de gevraagde aanpassingen te doen aan de persoonsgegevens, dan wel bepaalde Persoonsgegevens te verwijderen en vernietigen.

Artikel 10. Inschakelen van derden

10.1 De PRAKTIJK verleent aan CROSSUITE een algemene toestemming om subverwerkers aan te stellen met het oog op het uitvoeren van de verwerkingsactiviteiten die voorwerp uitmaken van onderhavige Verwerkersovereenkomst.

10.2 In geval CROSSUITE beroep wenst te doen op een subverwerker in de zin van dit artikel, verbindt CROSSUITE zich ertoe om met deze subverwerker een schriftelijke overeenkomst af te sluiten die minimaal de garanties en verplichtingen voortvloeiende uit deze Overeenkomst omvat.

10.3 CROSSUITE houdt een actueel register bij van de door hem ingeschakelde derden en subverwerkers waarin de identiteit, vestigingsplaats en een beschrijving van de werkzaamheden van de derden of subverwerkers zijn opgenomen, alsmede eventuele door de PRAKTIJK gestelde aanvullende voorwaarden. Dit register zal als bijlage 4 aan deze Verwerkersovereenkomst worden toegevoegd en zal door CROSSUITE actueel worden gehouden. Ingeval van een beoogde verandering van de subverwerkers, zal CROSSUITE de PRAKTIJK hier voorafgaandelijk van inlichten, waarbij de PRAKTIJK zich binnen de vijf werkdagen gemotiveerd en schriftelijk kan verzetten tegen deze verandering. Bij gebreke aan schriftelijk verzet binnen de voormelde termijn, wordt de PRAKTIJK verondersteld akkoord te gaan met de verandering.

Artikel 11. Aansprakelijkheid

11.1 CROSSUITE is louter verantwoordelijk voor de Verwerking van Persoonsgegevens via de door haar onder de Overeenkomst aangeboden dienst, onder de in de Verwerkersovereenkomst genoemde voorwaarden. Voor de overige Verwerkingen van Persoonsgegevens, waaronder in ieder geval begrepen maar niet beperkt tot de verzameling van de Persoonsgegevens door PRAKTIJK en/of derden, is CROSSUITE uitdrukkelijk niet verantwoordelijk.

11.2 De verantwoordelijkheid voor de doeleinden en de rechtmatigheid van de verwerking van de Persoonsgegevens die met gebruikmaking van een door CROSSUITE verleende dienst worden Verwerkt, ligt uitsluitend bij PRAKTIJK.

11.3 Indien CROSSUITE aangesproken wordt door de PRAKTIJK tot schadevergoeding ingevolge de niet naleving van deze Verwerkersovereenkomst of de toepasselijke wetgeving, dan zal de totale aansprakelijkheid van CROSSUITE beperkt zijn tot het totaal van de gefactureerde diensten in het vorige kalenderjaar, tenzij het bedrag waarvoor de bedrijfs- en/of beroepsaansprakelijkheid van CROSSUITE verzekerd is, lager is (tot 125.000 euro). Een reeks van samenhangende feiten wordt voor de toepassing van dit artikel als één gebeurtenis beschouwd.

11.4 CROSSUITE is niet aansprakelijk voor elke vorm van indirecte schade zoals, maar niet beperkt tot ondernemingsstagnatie, verminderde goodwill, gemiste besparingen, gederfde winst, reputatieschade of enige andere vorm van indirecte, incidentele of gevolgschade, ongeacht de aard van de handeling

11.5 Partijen zullen zich gedurende de Verwerkersovereenkomst adequaat verzekerd hebben en houden. De verzekeringsvoorwaarden hiertoe kunnen op verzoek worden ingezien.

Artikel 12. Geschillenregeling

12.1 Op de Verwerkersovereenkomst is uitsluitend het recht van het land waar CROSSUITE gevestigd is van toepassing

12.2 Alle geschillen die ontstaan naar aanleiding van deze Verwerkersovereenkomst worden beslecht op dezelfde wijze als opgenomen in de Overeenkomst.

Artikel 13. Voorrang

Op de Verwerkersovereenkomst is de Overeenkomst van toepassing. In het geval van eventuele tegenstrijdigheid tussen de (licentie)Overeenkomst en de Verwerkersovereenkomst, heeft het bepaalde in de Verwerkersovereenkomst voorrang.

BIJLAGE 1

A. Categorieën Betrokkenen

De personen waarop de Persoonsgegevens betrekking hebben zijn in ieder geval:

- patiënten
- huurders

B. Soort Persoonsgegevens

De Persoonsgegevens die door VERWERKER/CROSSUITE worden verwerkt zijn in ieder geval:

- NAW-gegevens, telefoonnummers, e-mailadres(sen)
- Vermelding zorgverzekeraar
- INSZ
- Beschrijving pathologie
- Geboortedatum
- Naam huisarts
- Beroep
- Hobby's en sport
- Familiesituatie

C. Aard en doel van de verwerking

De aard van de verwerking: ten behoeve van behandeling worden onderzoeks- gegevens en behandeljournaals gedocumenteerd.

De Persoonsgegevens worden in ieder geval voor de volgende doelen verwerkt:

Doeleinden van de verwerking:

- Verwerking met als doel een adequate behandeling te kunnen laten plaatsvinden, deze te monitoren en te evalueren;
- Verwerking met als doel de bereikbaarheid van patiënt en/of huisarts mogelijk te maken;
- Verwerking met als doel het maken van een afspraak voor behandeling van de patiënt.
- Verweking met als doel het in rekening brengen van de behandeling(en)
- Verwerking met als doel de kosten van de behandelingen(en) door te belasten aan zorgverzekeraar
- Verwerking met als doel, na instemming van de patiënt, verstrekken van een verslag, rapportage aan een derde.

Bijlage 2: Overzicht beveiligingsmaatregelen

Informatiebeveiliging- en privacybeleid

Er is een informatiebeveiligings- en privacybeleid dat voldoet aan de GDPR en eventuele richtsnoeren van de overheid en aansluit op de standaarden voor informatiebeveiliging ISO 27001 en NEN 7510. Dit beleid is intern gecommuniceerd en concreet geïmplementeerd door middel van gedocumenteerde procedures.

Certificering

Er is een managementsysteem voor informatiebeveiliging (ISMS). Dit managementsysteem is opgezet en ingericht conform de standaarden voor informatiebeveiliging ISO 27001 en NEN 7510. Het systeem is gecertificeerd door de onafhankelijke auditpartij Dekra.

Personeel

Medewerkers worden geïnformeerd over hun verantwoordelijkheden m.b.t. privacy en informatiebeveiliging en er wordt erop toegezien dat zij hun verplichtingen nakomen. Medewerkers die toegang hebben tot klant/patiëntgegevens zijn gebonden aan geheimhouding.

Contractmanagement (Sub)verwerkers

Met iedere toegestane (Sub)Verwerker wordt een verwerkersovereenkomst gesloten, die de (Sub)Verwerker contractueel verplicht tot nakoming van dezelfde verplichtingen in verband met de Verwerking als in de verwerkersovereenkomst.

Security incident & response

Er is een gedocumenteerd security incident response plan dat geschikt is om datalekken te detecteren, op te lossen en te melden, in overeenstemming met de verplichtingen in de verwerkersovereenkomst.

Versleuteling van gegevens in transit

Al het internetverkeer naar Crossuite verloopt via een SSL-versleutelde verbinding (Secure Socket Layer of veilige en beschermde overdracht van gegevens via het internet), en we aanvaarden enkel verkeer via poort 443.

Bij je eerste bezoek aan onze website verstuurt Crossuite een Strict Transport Security Header (HSTS) naar je browser. Daardoor is je verbinding voortaan volledig beveiligd via HTTPS of het veiligste internetprotocol. Zélfs als je op een niet-versleutelde link naar onze website klikt die specifiek begint met ‘http://’.

Patchmanagement / Netwerk- en systeembeveiliging

Er wordt periodiek beoordeeld of er kwetsbaarheden binnen de gebruikte applicaties, systemen en netwerken zijn. Patches en updates voor gevonden kwetsbaarheden worden doorgevoerd.

Crossuite maakt gebruik van Amazon Web Services (AWS) om data op te slaan. Deze servers ondergaan periodieke evaluaties zodat ze aan de nieuwste standaarden voldoen. Doordat we AWS als ons datacentrum gebruiken, is onze infrastructuur geaccrediteerd voor:

- ISO 27001
- SOC 1 en SOC 2/SSAE 16/ISAE 3402 (voorheen SAS 70 Type II)
- PCI Level 1
- C5 Operational Security
- ENS High
- IT-Grundschutz

Meer informatie over de beveiliging van AWS kan je hier terugvinden.

Wachtwoordbeleid en -opslag

Om je Crossuite-account aan te maken, moet je een sterk wachtwoord kiezen van ten minste 6 tekens. We slaan geen gebruikerswachtwoorden op in tekstvorm: we bewaren enkel niet-ontcijferbare wachtwoord-hashes die versleuteld werden met Bcrypt (inclusief per-user-random-salt). Op die manier beschermen we gebruikers tegen rainbow table-aanvallen en pogingen om de syntax voor versleuteling te ontcijferen.

Als een gebruiker meerdere keren (5x) een foutief wachtwoord ingeeft, vergrendelen we dit account om 'brute force'-aanvallen (manier om wachtwoorden te kraken via uitvoerige pogingen) te vermijden.
De gebruiker kan dan enkel opnieuw inloggen door een nieuw wachtwoord aan te vragen.

Om je account verder te beveiligen is er ook een Two-Factor Authentication (een extra beschermingslaag die enkel de gebruiker bezit) via gridcard, email, google Authenticator of sms.

Ons team gebruikt sterke, unieke wachtwoorden voor Crossuite-accounts en gebruikt Two-Factor Authentication voor elk apparaat en elke service. We moedigen onze medewerkers ook aan om password managers zoals LastPass te gebruiken om sterke wachtwoorden te genereren en op een veilige plaats te bewaren.

We versleutelen ook lokale harde schijven en schakelen automatische schermbeveiliging in.

Access management

De admin-functies van onze applicatie zijn slechts toegankelijk voor een selecte groep.
Gebruikerstoegang wordt tijdig ingetrokken of gewijzigd bij enige verandering in de status van personeel, leveranciers, Klanten, zakelijke partners of derden.

Fysieke toegangsbeveiliging

Er zijn passende maatregelen (zoals sloten, alarmsystemen) genomen om de ruimtes waarin de Persoonsgegevens kunnen worden Verwerkt, te beveiligen tegen onbevoegde toegang.

Logging

Er vindt logging plaats waarmee inzicht wordt verkregen in welke gebruikers wanneer zijn ingelogd, om na te kunnen gaan welke verwerkingen van Persoonsgegevens door welke gebruiker zijn uitgevoerd.

Applicatieontwikkeling – beveiligingsprincipes

Om alle veiligheidsnormen en -standaarden te respecteren, hanteren we strikte code reviews voor elke wijziging of toevoeging aan onze applicatie.

Bekendmaking van kwetsbaarheden (vulnerability disclosure)
Al sinds de lancering van Crossuite sporen we gebruikers actief aan om problemen in onze applicatie snel te melden, en zo de veiligheid en betrouwbaarheid van ons platform te helpen waarborgen. Alle meldingen behandelen en beantwoorden we zo snel mogelijk.

Bijlage 3: Overzicht van inlichtingen bij een incident

CROSSUITE verschaft in ieder geval de volgende informatie aan de PRAKTIJK bij een incident die persoonsgegevens van verwerkingsverantwoordelijke betreft:

- wat de (vermeende) oorzaak is van de inbreuk;
- wat het (vooralsnog bekende en/of te verwachten) gevolg is;
- wat de (voorgestelde) oplossing is;
- contactgegevens voor de opvolging van de melding;
- aantal personen waarvan gegevens betrokken zijn bij de inbreuk (indien geen exact aantal bekend is: het minimale en maximale aantal personen waarvan gegevens betrokken zijn bij de inbreuk);
- een omschrijving van de groep personen van wie gegevens betrokken zijn bij de inbreuk;
- het soort of de soorten persoonsgegevens die betrokken zijn bij de inbreuk;
- de datum waarop de inbreuk heeft plaatsgevonden (indien geen exacte datum bekend is;
- de periode waarbinnen de inbreuk heeft plaatsgevonden);
- de datum en het tijdstip waarop de inbreuk bekend is geworden bij verwerker of bij een door hem ingeschakelde derde of Subverwerkers;
- of de gegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk zijn gemaakt voor onbevoegden;
- wat de reeds ondernomen maatregelen zijn om de inbreuk te beëindigen en om de gevolgen van de inbreuk te beperken.

Bijlage 4: overzicht van de subverwerkers

Subverwerker 1:	Bart.SK SRO
Beschrijving van de werkzaamheden	Resource partner

Subverwerker 2:	LINK Mobility Sp. z o.o.
Beschrijving van de werkzaamheden	Versturen sms'en

Subverwerker 3:	AWS Europe
Beschrijving van de werkzaamheden	Hosting partner

Subverwerker 4:	Stripe
Beschrijving van de werkzaamheden	Betalingsverwerking