ruler

In control.

Ruler Hosting & Security

2020-2021

Inhoudsopgave

	Pagenumber
1. Introductie	3
2. Structuur van de applicatie	4
3. Ontwikkeling, onderhoud en beheer van de software	5
4. Hosting platform	6
5. Certificeringen	7
6. Privacy en GDPR	10
7. Waar wordt uw date opgeslagen?	11
8. Escrow	12
9. Toegepaste best practices voor informatiebeveiliging	13

1 Introductie

Door de toenemende digitalisering van de samenleving is het zorgvuldig omgaan met de informatie en gegevens van organisatie en hun ketenpartners van groot belang. Ruler beseft terdege dat uitval van computers of telecommunicatiesystemen, het manipuleren van gegevens, het in ongerede raken van gegevensbestanden of het door onbevoegden kennisnemen van uw gegevens, ernstige gevolgen voor uw organisatie kan hebben.

Als initiatiefnemer in Europa heeft De Nederlandse Bank er in 2012 voor gezorgd dat het wettelijk mogelijk werd voor organisaties in sterk gereguleerde bedrijfstakken, zoals banken, verzekeraars en nutsbedrijven, om te kunnen outsourcen naar de Cloud. Cloud leveranciers zoals Microsoft, hebben op hun beurt daarop gereageerd door instellingen die gebruik willen gaan maken van hun diensten, contracten voor te leggen waarin o.a. het onderzoeksrecht van DNB, het zogenoemde 'right to examine', is opgenomen.

Voor Ruler staat veiligheid voorop. Ruler maakt daarom maximaal gebruik van de beveiligingsmaatregelen zoals die door Microsoft binnen het Azure Cloud platform worden geboden. Maatregelen die aansluiten op de eisen en wensen van de financiële sector. Zo blijft uw data binnen Europa en kunt u voldoen aan alle relevante wet- en regelgeving.

2 Structuur van de applicatie

De Ruler applicatie is opgebouwd uit twee onderdelen:

- De back-end api die communicatie met de database beheert en hierover alle nodige authenticatie en autorisatie checks uitvoert om te waarborgen dat alleen bevoegden toegang krijgen tot de data.
- De front-end applicatie die is ontwikkeld om de eindgebruiker zo goed mogelijk te faciliteren in zijn/haar interacties met de applicatie.

Beide onderdelen zijn geprogrammeerd in Typescript (type safe Javascript) om ervoor te zorgen dat het aantal bugs in het systeem geminimaliseerd wordt. De front-end maakt gebruikt maakt van React framework en de back-end api gebruik maakt van Node.js. We maken gebruik van GraphQL als taal om tussen de backend en de frontend te communiceren. GraphQL dient als integratielaag om ook gemakkelijk te kunnen integreren met andere REST API's. De applicaties worden via continuous integration gebuild naar Docker images.

Ruler wordt ontwikkeld volgens het agile principe en heeft daardoor een zeer hoge iteratiesnelheid. Hierdoor kunnen security patches in de bovengenoemde softwarematige afhankelijkheden snel worden meegenomen en blijft Ruler altijd up-to-date met de laatste beveiligings updates.

We werken samen met security-partij RadicallyOpenSecurity, die op aanvraag pentests op de systemen uitvoeren. Onze technische stack wordt door hen in een rapport als volgt lovend beschreven: "The source repositories were well shaped and clearly structured. The overall quality appeared to meet requirements of modern software development and security best-practices."

We maken gebruik van Azure Database for PostgreSQL (https://azure.microsoft.com/en-us/services/postgresql/) als database waarmee de back-end communiceert om gestructureerde data op te slaan. Van de PostgreSQL database wordt regelmatig (meerdere keren per dag) een backup van gemaakt. Backups worden, waar van toepassing, altijd encrypted, zowel in-transit (SSL / https) als in-rest.

We maken gebruik van Azure Storage wordt om binaire data op te slaan (https://azure.microsoft.com/en-us/services/storage/?v=18.24). Dit gebeurt zowel versleuteld door de back-end als door Azure Storage zelf op het moment van schrijven naar de onderliggende data opslag (SSD). Ook hier wordt regelmatig een backup van gemaakt.

3 Ontwikkeling, onderhoud en beheer van software

De Ruler applicatie wordt (door-) ontwikkeld, onderhouden en ondersteund door Lifely B.V. Binnen het Lifely team zijn alle technische disciplines voor de ontwikkeling van een online applicatie aanwezig, waaronder interface en interactie ontwerp, apps (native), front-end, back-end en cloud services. Het development team wordt aangevuld met specialisten op het gebied van design, user experience, architectuur en security.

Voor meer informatie over Lifely, zie: https://lifely.nl.

Lifely voert een aantal systeembeheer taken uit op het platform waarop Ruler draait. Microsoft gaat er ook vanuit dat haar klanten deze taken zelf uitvoeren. Het gaat om de volgende taken:

- Aanvragen, verlengen en intrekken van SSL certificaten en domeinnamen;
- Bepalen, instellen en controleren van firewall regels voor verkeer tussen zones, zowel voor de applicatie als de beheerde databases;
- Periodieke controle van toegangslogboeken;
- Afstemmen en uitvoeren van een eventuele herstelactie vanaf een back-up met de beheerders van Microsoft Azure;
- Plannen, testen en initiëren van een eventuele uitwijkprocedure;
- Monitoring van de status (beschikbaarheid, prestaties, capaciteit) van het Microsoft Azure hosting platform.
- Periodiek checken en implementeren van suggesties zoals gegeven door de Azure Advisor, zie ook https://azure.microsoft.com/en-us/services/advisor/.

4 Hosting platform

Indien u gebruik maakt van Ruler, maakt u indirect gebruik van Microsoft Azure als hosting-platform. Microsoft Azure bestaat uit een uitgebreide verzameling van clouddiensten waarmee ontwikkelaars - zoals Lifely - toepassingen bouwen, implementeren en beheren in het wereldwijde netwerk van datacenters van Microsoft. De hosting-overeenkomst is afgesloten tussen Lifely B.V. en Microsoft Ireland Operations Ltd. (hierna: Microsoft Azure).

Microsoft Azure voldoet aan de hoogste standaarden van beveiliging van clouddiensten. De data wordt opgeslagen in het Microsoft datacenter in Amsterdam (Regio: West-Europe). Voor veel meer aspecten van beveiliging binnen Microsoft Azure verwijzen we naar: https://azure.microsoft.com/nl-nl/services/security-center/

5 Certificaten

De Microsoft Azure clouddiensten behoren tot de best beheerde en meest veelvuldig en breed gecertificeerde Cloud-omgevingen ter wereld. Dit geeft klanten de zekerheid dat Microsoft Azure op een groot aantal thema's en invalshoeken ruimschoots – vaak meer dan ruimschoots – voldoet aan wet- en regelgeving, industrie-standaarden en best practices. Dit wordt vele malen per jaar door toezichthouders, accountants en auditors getoetst. Microsoft maakt deze auditverslagen ook beschikbaar voor klanten, zodat u zelf kennis kunt nemen van de bevindingen van auditors, eventuele tekortkomingen en de herstelacties die gedefinieerd zijn. Microsoft maakt het mogelijk en biedt u de randvoorwaarden dat u, ongeacht uw bedrijfstak en uw toepassing, kunt voldoen aan alle wet- en regelgeving die op uw situatie van toepassing is.

In de onderstaande tabel staat een overzicht van een deelverzameling van de door Microsoft Online Services behaalde certificaten. Het gaat vooral om certificaten die internationaal en op Europees niveau relevant zijn.

Standaard en beschrijving

BIR 2012
Agencies operating in the Netherlands government sector must comply with the Baseline Informatiebeveiliging Rijksdienst standard.

EN 301 549
Microsoft meets EU accessibility requirements for public procurement of ICT products and services.

ENISA IAF
Azure aligns with the ENISA framework requirements through the CSA CCM version 3.0.1.

European Union Model Clauses
Microsoft offers EU Standard Contractual Clauses, guarantees for transfers of personal data.

EU-U.S. Privacy Shield
Microsoft complies with this framework for protecting personal data transferred from the EU to the US.

FACT
Microsoft Azure achieved certification from the Federation Against Copyright Theft in the UK.

IT Grundschutz Compliance
Azure Germany published this Workbook to help our clients achieve IT Grundschutz certification.

NEN 7510:2011
Organizations in the Netherlands must demonstrate control over patient health data in accordance with the NEN 7510 standard.

NHS IG Toolkit
Azure is certified to the Health Information Trust Alliance Common Security Framework.

Spain ENS
Microsoft received Spain's Esquema Nacional de Seguridad (National Security Framework) certification.

UK Cyber Essentials PLUS
Cyber Essentials PLUS is a UK government-defined scheme to help organizations protect against common cyber-security threats.

UK G-Cloud
The Crown Commercial Service renewed the Microsoft cloud services classification to Government Cloud v6.

CDSA
Azure is certified to the Content Delivery and Security Assoc. Content Protection and Security standard.

CSA STAR Attestation
Azure and Intune were awarded Cloud Security Alliance STAR Attestation based on an independent audit.

GxP
Microsoft cloud services adhere to Good Clinical, Laboratory, and Manufacturing Practices (GxP).

ISO 9001:2015 Quality Management Systems Standards
Microsoft is certified for its implementation of these quality management standards.

ISO/IEC 20000-1:2011 Information Technology Service Management
Microsoft is certified for its implementation of these service management standards.

ISO 22301:2012 Business Continuity Management Standard
Microsoft is certified for its implementation of these business continuity management standards.

ISO/IEC 27001:2013 Information Security Management Standards
Microsoft is certified for its implementation of these information security management standards.

ISO/IEC 27017:2015 Code of Practice for Information Security Controls
Microsoft cloud services have implemented this Code of Practice for Information Security Controls.

ISO/IEC 27018 Code of Practice for Protecting Personal Data in the Cloud
Microsoft was the first cloud provider to adhere to this code of practice for cloud privacy.

MPAA
Azure successfully completed a formal assessment by the Motion Picture Association of America.

Shared Assessments
Microsoft demonstrates alignment of Azure with this program through the CSA CCM version 3.0.1.

SOC 1
Microsoft cloud services comply with Service Organization Controls standards for operational security.

SOC 2
Microsoft cloud services comply with Service Organization Controls standards for operational security.

SOC 3
Microsoft cloud services comply with Service Organization Controls standards for operational security.

WCAG 2.0
Microsoft cloud services comply with the Web Content Accessibility Guidelines 2.0.

6 Privacy en GDPR

Microsoft is de eerste Cloud-provider die voldoet aan de ISO/IEC 27018 standaard, ontwikkeld door de ISO, als internationaal geldende normering voor de bescherming van persoonsgegevens die in de Cloud zijn opgeslagen. Het British Standards Institute (BSI) heeft in een onafhankelijk onderzoek vastgesteld dat Microsoft Azure voldoet aan de vastgestelde regels voor de bescherming van persoonsgegevens (PII) in de public Cloud. Het belang van het voldoen aan de ISO 27018 normering is dat het zakelijke klanten garandeert dat privacy in de Microsoft cloud op verschillende manieren beschermd is. Microsoft is hiermee ook compliant voor haar verplichtingen inzake de GDPR, die vanaf 25 mei 2018 geldig is.

Het uitgangspunt is dat de klant de controle behoudt over de eigen (persoons-) gegevens, Microsoft verwerkt persoonlijk herleidbare gegevens uitsluitend volgens de instructies die de klant verstrekt. Ook weet de klant wat er met zijn data gebeurt. Microsoft houdt zich aan strikte regels met betrekking tot het retourneren, overdragen en vernietigen van persoonlijke informatie die in haar datacenters zijn opgeslagen. Microsoft informeert de klant niet alleen waar zijn data staat, maar ook wanneer politie, justitie of veiligheidsdiensten toegang tot bepaalde gegevens willen. Ook wordt de klant direct geïnformeerd wanneer er sprake is van ongeautoriseerde toegang tot persoonlijke gegevens, verwerkingsapparatuur of systemen die resulteren in het verlies, openbaarmaking of veranderingen in deze informatie.

Ook biedt Microsoft en aantal belangrijke veiligheidsgaranties, zoals specifiek restricties die gelden bij het omgaan met persoonlijke gegevens, het verzenden ervan via openbare netwerken, het opslaan op draagbare media en het volgen van de juiste procedures bij eventuele datarecovery en herstel. De standaard bepaalt tevens dat alle personeel dat toegang heeft tot, c.q. omgaat met persoonlijke gegevens, verplicht is om deze vertrouwelijk te houden. Dat houdt tevens in dat persoons- en persoonlijke gegevens niet voor commerciële doeleinden worden gebruikt, een regel waar niet alle serviceproviders zich aan houden. Wanneer overheidsinstanties toegang eisen tot bepaalde data van klanten moet dat voornemen volgens de ISO-norm aan zakelijke klanten worden gemeld, tenzij daar wettelijke bezwaren tegen bestaan.

Uit de analyse van de voorwaarden van Microsoft blijkt dat zij uitgebreide technische en organisatorische maatregelen genomen heeft en juridische waarborgen geeft voor een veilige omgang met (persoons-) gegevens. Dit blijkt ook uit de verschillende (internationale) onafhankelijke audits en certificeringen (zoals ISO 27001).

7 Waar wordt uw data opgeslagen?

De data in Ruler wordt opgeslagen in het Microsoft datacenter in Amsterdam (Regio: West-Europe).

Hierbij merken wij op dat de primaire locatie Amsterdam is maar dat in geval van calamiteiten er een uitwijk mogelijk is binnen Europa (Dublin en/of Berlijn).

Ruler heeft bewust gekozen voor de Azure omgeving vanwege de beveiliging en de data storage in West-Europa. Voor de specifieke data storage services in West-Europa betaalt Ruler een aanvullende fee aan Azure.

Dat Microsoft de data die zij beheert niet zomaar vrijgeeft, blijkt onder andere uit een aantal rechtszaken die momenteel lopen tussen Microsoft en de Ierse overheid enerzijds en de Amerikaanse justitie anderzijds. Deze heeft gegevens opgevraagd die opgeslagen staat in Dublin, Ierland. U ziet dat deze informatie dus niet zomaar gedeeld wordt, zoals vaak wel wordt aangenomen.

8 Escrow

Om de continuïteit van onze dienstverlening naar u te allen tijde te garanderen heeft Ruler zich verplicht tot het opzetten en onderhouden van een deugdelijke broncode escrow regeling ten behoeve van de afnemer. De broncode escrow regeling is door Ruler opgezet in samenwerking met de Software Borg Stichting te Haren. De afnemer van Ruler heeft op grond van de broncode escrow regeling onder voorwaarden recht op de broncode van de Programmatuur voor continuïteitsdoeleinden. Als additionele maatregel is het intellectueel eigendom en de broncode ondergebracht bij een separate rechtspersoon: Tooler B.V.

9 Toegepaste best practices voor informatiebeveiliging

In de onderstaande tabel treft u een overzicht aan van de toegepaste ‘best practice’ informatie-beveiligingsmaatregelen in de Azure hosting-omgeving.

Onderdeel	Hoe geïmplementeerd
Authenticatie van eindgebruikers Authenticatie vindt plaats op het niveau van eindgebruikers, in de gehele keten	Voor toegang tot de applicatie is altijd en overal authenticatie vereist. Standaard werkt Ruler met een login gebaseerd op een gebruikersnaam en een wachtwoord. De benodigde technische voorzieningen daarvoor zijn onderdeel van het Microsoft Azure platform. De Ruler applicatie maakt gebruik van deze voorzieningen.
Centrale administratie identiteiten Identiteiten, rollen en grofmazige autorisaties worden centraal geadministreerd	De klant bepaalt zelf wie als beheerder of als gebruiker toegang heeft tot (de gegevens in) Ruler. Deze gebruikers worden in een centrale database met gebruikersgegevens vastgelegd. De database is beschikbaar als onderdeel van het Microsoft Azure hosting platform. De Ruler applicatie maakt gebruik van deze voorzieningen.
Centrale auditlog Beveiligings-gerelateerde gebeurtenissen worden vastgelegd in een centraal logboek.	Alle toegang door iedere beheerder of gebruiker tot functies en gegevens in de applicatie wordt gelogd. De Ruler applicatie legt alle toegangscontrole- en beveiligings- gerelateerde gebeurtenissen vast in de auditlogs. Azure Log Analytics centraliseert logboekgegevens van meerdere systemen in één gegevensopslag. Het zet activiteiten en gegevens over resources voor verschillende abonnementen naast elkaar om inzichten te verkrijgen waarop Ruler direct actie kan ondernemen. Periodiek wordt door Lifely een controle uitgevoerd of ongeautoriseerde toegang heeft plaatsgevonden.

Continue en proactief bewaken serviceniveaus De serviceniveaus van IT-systemen worden continu en proactief bewaakt	Buiten alle tools die beschikbaar zijn binnen het Azure platform die worden ingezet om serviceniveaus te waarborgen, wordt er door Lifely gebruik gemaakt van externe monitoring en analyse tools om continue en onafhankelijk van Microsoft de status van het Azure platform en Ruler te monitoren.
Dagelijkse back-up Van alle gegevens wordt minimaal dagelijks een back-up gemaakt	Microsoft garandeert voor kritische onderdelen van het Azure platform een beschikbaarheid van tenminste 99,95%. Hiertoe maakt Microsoft o.a. dagelijks meerdere back-ups. Zowel om aan haar service-level verplichtingen naar Ruler te kunnen voldoen, als ook op verzoek van Ruler zelf, zal Microsoft een back-up terugzetten. Dit gaat altijd in onderling overleg.
Beveiligen onderlinge verbindingen Het netwerk is ingedeeld in zones met filtering op de zonegrenzen	Firewalls zorgen voor de filtering van het verkeer tussen de zones. Hierdoor worden individuele componenten in de architectuur van Ruler onderling verbonden op een manier waarop zij van buiten niet toegankelijk zijn. Denk hierbij aan de connectie tussen de applicatie en de database. Het beheer van deze regels valt onder de verantwoordelijkheid
Geauthentiseerde en geautoriseerde toegang Toegang tot IT systemen wordt geauthentiseerd en geautoriseerd	Alle toegang tot autorisatie-objecten binnen Ruler wordt expliciet geauthenticeerd en geautoriseerd. De logingegevens worden gevalideerd op basis van de in de database opgeslagen gebruikersprofielen. Voor alle autorisatie-objecten is aangegeven welke rollen of gebruikers geautoriseerd toegang kunnen krijgen.
Geautomatiseerd beheer Het beheer van IT systemen is zoveel mogelijk geautomatiseerd	Duizenden grotere en kleinere operationele processen, zoals het aanmaken van nieuwe klantaccounts, het instellen en controleren van toegangsrechten, het actief maken of uitbreiden van services, de facturatie voor een klant, het uitvoeren van een disaster recovery procedure, het controleren van back-ups en het uitvoeren van security scans en compliance audits, zijn bij Microsoft Azure volledig geautomatiseerd. Die automatisering en de hoge mate van standaardisatie binnen Azure hebben niet alleen positieve gevolgen voor snelheid en doorlooptijd, maar zeker ook voor de veiligheid, kwaliteit en voorspelbaarheid van de service-processen door de kans op menselijke fouten, misbruik en sabotage tot het absolute minimum terug te brengen.

Hardening beveiligingscomponenten Componenten die een beveiligingsfunctie vervullen zijn gehardened	Systeem-hardening in het MS Azure platform is gebruikt om zo veel mogelijk veiligheidsrisico's te elimineren. Dit wordt over het algemeen gedaan door overbodige functies en/of software van het besturingssysteem uit te zetten of van het systeem te verwijderen. Denk daarbij aan het uitschakelen of verwijderen van onnodige gebruiker-accounts en systeemservices, het aanscherpen van het wachtwoordbeleid, de toegang tot bestanden en directories, systeemrechten, kernel-parameters, netwerkinstellingen en het patchbeleid. Hardening is nodig om de toegang tot een systeem zo moeilijk mogelijk te maken. En, als het een aanvaller dan toch lukt om toegang te krijgen, dan is het systeem zodanig gelimiteerd dat die aanvaller bijzonder weinig kan uitrichten. Deze hardening moet bewaakt worden en regulier ge-audit worden. De hiervoor vermelde volledig geautomatiseerd processen zorgen hiervoor.
Herleidbaarheid van handelingen Gebruik van IT-systemen is herleidbaar naar gebruikers	Microsoft berekent bij Azure, net zoals veel andere Cloud providers, voor het gebruik van het platform op basis van 'pay-per-use'. Om die reden heeft Microsoft voorzien in instrumentatie, die ieder gebruik van services en resources, door iedere gebruiker, op alle momenten van de dag meet. Deze gegevens worden niet alleen gebruikt voor facturatie maar dienen ook om inzicht te krijgen in de gebruikspatronen. Daarmee zijn alle handelingen en gebruik van diensten en resources 'zichtbaar' geworden en kunnen deze ook voor informatiebeveiligings-doeleinden gebruikt worden.
Hoge beschikbaarheid basisinfrastructuur De basisinfrastructuur is hoog beschikbaar.	Microsoft garandeert voor sommige van de individuele bouwstenen van het Azure platform een beschikbaarheid van tenminste 99,95%. Het Azure platform is gekoppeld aan netwerken met meervoudige verbindingen en hardware. Aan de hand van die bouwstenen en verbindingen is door Lifely een systeemontwerp gemaakt dat maximale beschikbaarheid moet garanderen, uitval van meerdere componenten kan weerstaan en maximaal gebruik van de beschikbare resources kan leveren.

Laagste toegangsrechten Toegangsrechten moeten zijn gebaseerd op wat nodig is voor het uitoefenen van de functie (Least Privilege).	Standaard zijn in Ruler voor de verschillende rollen alleen die rechten toegekend, die nodig zijn voor het uitvoeren van de bij de rol behorende taken. Bij de eerste ingebruikname van Ruler start uw omgeving met de standaardinstellingen. De autorisaties van uw eigen gebruikers kunnen (verder) worden beperkt. Indien u specifieke wensen heeft omtrent autorisatieprofielen dan is het mogelijk deze in Ruler aan te passen.
Meerdere beveiligingsstrategieën Beveiliging is end-to-end en gebaseerd op meerdere defensieve strategieën	Door het gebruik van virtuele machines van het Azure platform, kan Ruler een gelaagde beveiligingsarchitectuur bieden op verschillende niveaus van het netwerk en voor elke toepassings-laag.
OTAPU Ontwikkel-, test-, acceptatie-, productie- en uitwijk- omgevingen zijn gescheiden	Als klant heeft u uitsluitend te maken met de productieomgeving van Ruler. Lifely hanteert bij de ontwikkeling van nieuwe updates een strikte scheiding tussen de verschillende omgevingen. Ook productie- en uitwijk-omgevingen zijn gescheiden, maar in dit geval wel identiek.
Password policy Wachtwoorden conformeren aan een standaard password policy	Als klant bent u zelf verantwoordelijk voor het vaststellen van uw eigen wachtwoordbeleid. De Ruler applicatie kan uw vastgesteld wachtwoordbeleid vervolgens wel afdwingen, bijvoorbeeld door te controleren op wachtwoordlengte, hergebruik van wachtwoorden en complexiteit van het door de gebruiker gekozen wachtwoord. Eventueel kunt u als extra beveiliging naast gebruikersnaam en wachtwoord ook gebruik maken van een one-time password (OTP) of een smartcard. Wij informeren u graag over de mogelijkheden.
Patching Patches worden periodiek beoordeeld en kritische patches worden snel toegepast	Microsoft is bij de levering van een groot deel van haar services verantwoordelijk voor het uitvoeren van patchmanagement, dus voor het operating systeem, device drivers, databases, web server, networking en firewalls. Kortom alles, met uitzondering van de eigenlijke Ruler applicatie.

Serviceniveauovereenkomsten Er zijn serviceniveauovereenkomsten met externe beheerders van applicaties en infrastructuur	In de Serviceniveauovereenkomsten biedt Microsoft garanties voor beschikbaarheid voor afzonderlijke services. Microsoft garandeert een beschikbaarheid van tenminste 99,95% per maand voor door Ruler gebruikte services. Lifely heeft op basis van de afzonderlijke services een systeemontwerp gemaakt dat maximale beschikbaarheid van de Ruler applicatie kan garanderen, uitval van meerdere componenten kan weerstaan en maximaal gebruik van de beschikbare resources kan leveren. De beschikbaarheid van Ruler ligt in de praktijk wat hoger dan die van de afzonderlijke systeemcomponenten, maar Lifely kan deze niet garanderen.
Encryptie van data Zowel tijdens transport als bij opslag wordt encryptie van data toegepast	De site van Ruler heeft een beveiligingscertificaat. Alle communicatie van de browser tot aan het Azure platform is tijdens transport versleuteld en dus niet door derden in te zien. Het Azure platform versleuteld ten allen tijden data 'at rest' zodat bij inbreuk in de onderliggende infrastructuur geen gegevens lekken. Buiten het versleutelde verkeer en data opslag die aangeboden worden door het Azure platform, versleutelt de Ruler applicatie zelf een aantal data punten in het systeem om er zeker van te zijn dat uw data niet inzichtelijk wordt voor derden.
Wachtwoorden onleesbaar Wachtwoorden kunnen door niemand gelezen worden	Wachtwoorden worden nooit ‘plain text’ over het netwerk verstuurd of opgeslagen op het platform. Sterke encryptie wordt toegepast om de wachtwoorden en gebruikersprofielen op te slaan.
Hardware	Laptops/harddrives van al onze ontwikkelaars en designers zijn encrypted.
Code reviews	Server code die gerelateerd is aan authenticatie of autorisatie van data wordt altijd strikt via het vier-ogen principe en peer reviews gecontroleerd.