

## SERVICE LEVEL AGREEMENT (SLA)

### 1. Algemeen

Deze Service Level Agreement (SLA) heeft betrekking op het gebruik van Diensten op basis van een Gebruikersovereenkomst tussen Leverancier en Afnemer. De SLA dient in samenhang met de Gebruikersovereenkomst en Algemene Voorwaarden Diensten begrepen te worden. In de SLA zijn de wederzijdse verplichtingen en inspanningen ter zake de Dienst vastgelegd.

### 2. Definities

- Leverancier: Verzuim Onder Controle B.V., ingeschreven onder KvK nr 17270928.
- Afnemer: gebruiker van en contractuele wederpartij ter zake door Leverancier geleverde diensten.
- Dienst: Leverancier stelt en houdt voor de Afnemer een verzuimregistratiesysteem via het Internet beschikbaar. De online applicatie bestaat uit verschillende modules, welke worden gespecificeerd in de Gebruikersovereenkomst.
- Gebruikersovereenkomst: voor elke Dienst die Afnemer wenst te gebruiken, worden in een specifieke overeenkomst voor de te leveren Dienst de tarieven e.d. vastgelegd.
- Service Window: tijdspanne waarbinnen de Dienst beschikbaar is: 24 uur per dag, 7 dagen per week.
- Sessie: aanmelding bij de Dienst waarna de Dienst kan worden gebruikt. Een sessie eindigt wanneer de gebruiker uitlogt of automatisch één uur na de laatste interactie met de Dienst.
- Secure Socket Layer (SSL): algemeen gebruikt internetprotocol dat zorgt voor beveiligde verbindingen.
- Server: computer die binnen een netwerkgegevens opslaat en verwerkt ten behoeve van meerdere cliëntcomputers.
- Firewallstelsel: bescherming van computers en netwerken van computers middels controle van in- en uitgaand (data)verkeer.
- Incident: probleem in de Dienst dat oplossing behoeft.
- Reactietijd: tijd tussen aanmelden van een incident en 1ste reactie van Leverancier.
- Oplossingstijd: tijd tussen aanmelden incident en oplossing van het incident.

### 3. Verplichtingen

Onderstaande verplichtingen gelden onverminderd de verplichtingen zoals beschreven in de Algemene Voorwaarden Diensten.

#### 3.1 Afnemer draagt zorg voor:

- hard- en software op de werkplek
- infrastructuur en beveiliging binnen de eigen organisatie
- verbinding met het Internet
- invoer van gegevens
- bescherming van toegangsmiddelen
- zorgplicht t.a.v. gebruik van de Dienst
- privacy-bewustzijn (conform Wbp en AVG)
- updates van personeelsgegevens vinden alleen via de portal plaats (nooit via e-mail).

#### 3.2 Leverancier draagt zorg voor:

- verschaffen van toegang; verstrekken van codes en instructies
- beschikbaarheid van de Dienst
- beveiliging van de Dienst
- ondersteuning van Afnemer

3.3 Op verzoek van Afnemer kan Leverancier Afnemer adviseren ter zake de inrichting en beveiliging van werkstations en infrastructuur. Leverancier en Afnemer zullen daartoe in voorkomend geval een aanvullende overeenkomst aangaan.

### 4. Beschikbaarheid en onderhoud

4.1 Uitgangspunt is continue beschikbaarheid van de Dienst. Leverancier zal de Dienst in ieder geval gedurende het Service Window aan Afnemer ter beschikking stellen. Leverancier streeft naar een minimale beschikbaarheid van 99% gedurende deze periode.

4.2 Teneinde de beschikbaarheid van de Dienst te realiseren, zijn de systemen van Leverancier voorzien van een dubbel uitgevoerde noodstroomvoorziening, waarmee stroomonderbrekingen van het openbare net worden opgevangen.

4.3 De Dienst dient (preventief) onderhouden te worden. Leverancier zal het (preventief) onderhoud waar mogelijk buiten de in 4.1. genoemde tijdspanne verrichten.

4.4 De tijd dat de Dienst niet beschikbaar is als gevolg van (preventief) onderhoud, strekt niet in mindering op de beschikbaarheid als bedoeld in artikel 4.1.

### 5. Beveiliging

5.1 De Dienst draait op systemen van het Datacenter. Deze systemen zijn geplaatst in een omgeving die te allen tijde op meerdere niveaus van toegangsbeveiliging zijn voorzien. Uitsluitend geautoriseerde personen krijgen toegang tot deze omgeving.

5.2 De omgeving is voorzien van brand en inbraak werende middelen.

5.3 Leverancier zal vergaande maatregelen treffen om beïnvloeding van de Dienst door virussen e.d. alsmede onbevoegde benadering en gebruik tegen te gaan.

5.4 Het is niet toegestaan de Dienst en bijbehorende mailservers voor SPAM-doeleinden te gebruiken.

5.5 Leverancier behoudt zich in verband met de beveiliging van de Diensten en het anti-SPAM-beleid het recht voor de toegang van één of meer Afnemers te blokkeren. In voorkomende gevallen zal Leverancier de betreffende Afnemer hieromtrent zo spoedig mogelijk informeren.

5.6 Het niet nakomen van de in artikel 3.1 genoemde verplichtingen kan reden zijn de toegang te blokkeren.

### 6. Toegangsbeveiliging en integriteit

6.1 Leverancier maakt aan iedere Afnemer unieke gebruikersnamen met bijbehorende wachtwoorden bekend.

6.2 Afnemer mag een gebruikersnaam slechts vanaf één werkstation met één aanmelding tegelijkertijd gebruiken.

6.3 Indien Afnemer tegelijkertijd meerdere Sessies heeft aangemeld, neemt Afnemer het risico van verlies of onjuiste verwerking van data.

6.4 Slechts Afnemer en de daartoe geautoriseerde systeembeheerders kunnen wachtwoorden wijzigen.

6.5 De systeemdata is inhoudelijk van buiten het systeem van Leverancier slechts toegankelijk voor Afnemer. Afnemer kan de systeemdata toegankelijk maken voor andere gebruikers. Afnemer is dan zelf verantwoordelijk voor de integriteit van de data alsmede voor het informeren omtrent de toegang en het gebruik van de Dienst. Omwille van beveiliging en privacy kan Leverancier anderen dan Afnemer niet informeren.

6.6 De koppeling tussen Afnemer en de Dienst kan slechts tot stand worden gebracht middels een Secure Socket Layer (SSL). Dat betekent dat ingevulde gegevens versleuteld worden verstuurd, en niet door derden kunnen worden gelezen. Wachtwoorden worden ook versleuteld opgeslagen en kunnen noch door Leverancier, noch door buitenstaanders worden achterhaald.

6.7 De toegang tot het centrale systeem staat onder controle van een Firewallstelsel. Slechts door het Firewallstelsel toegestane toegang en activiteiten kunnen worden uitgevoerd.

6.8 Servers van Leverancier staan fysiek in een ISO 27001 gecertificeerd datacenter (ISO-standaard voor informatiebeveiliging) in de EU en zijn niet onderhevig aan de zogenoemde Amerikaanse Patriot Act.

6.9 Leverancier zal de persoons- of bedrijfsgegevens van Afnemer strikt vertrouwelijk behandelen. Tenzij Leverancier op grond van de wet of een rechterlijke uitspraak daartoe is verplicht, zal Leverancier de gegevens niet aan derden ter beschikking stellen.

6.10 Persoons- of bedrijfsgegevens van Afnemer worden alleen via een beveiligd portaal uitgewisseld en opgeslagen in versleutelde databases. Het ontsleutelen van de databasegegevens vereist een encryptiesleutel die alleen op Server in een beveiligd netwerk staat. De gegevens in de databases zijn zonder de encryptiesleutel niet leesbaar.

### 7. Back-up

7.1 Leverancier maakt dagelijks een back-up van de aanwezige data op haar systemen.

7.2 Alleen voor bestanden die sinds de laatste back-up zijn veranderd vindt een nieuwe back-up plaats (incremental back-up).

### 8. Ondersteuning

8.1 Aan Afnemer staat kosteloos een helpdesk ter beschikking voor ondersteuning van de in verband met de Dienst te gebruiken applicatie- en systeemsoftware.

8.2 De helpdesk van Leverancier is op werkdagen van 9:00u tot 17:00u bereikbaar. Op nationale vrije dagen is de helpdesk gesloten.

De helpdesk van Leverancier is de gehele dag bereikbaar per email: [support@verzuimondercontrole.nl](mailto:support@verzuimondercontrole.nl).

8.3 Ondersteuning vindt plaats op werkdagen van 9:00u tot 17:00u.

8.4 De reactietijd van incidenten bedraagt maximaal 1 uur binnen kantooruren. De periode buiten de in artikel 4.1 genoemde periode geldt niet als reactietijd.

8.5 De oplossingstijd van incidenten bedraagt in beginsel maximaal 4 uur binnen kantooruren. De periode buiten de in 4.1 genoemde periode geldt niet als oplossingstijd.

8.6 In geval de melding geen incident (b)lijkt te betreffen of als er sprake is van verstoring van de Dienst door overmacht gerelateerd aan virussen, wormen of hardware defecten e.d., streeft Leverancier in beginsel naar een oplossingstijd van maximaal één werkdag.

8.7 Wanneer de oplossingstijd van de verstoring naar verwachting langer dan de aangegeven tijdspanne zal bedragen, zal Leverancier Afnemer hieromtrent zo spoedig mogelijk informeren.

### 9. Diversen

9.1 Leverancier streeft naar continuïteit van de applicatie- en systeemsoftware. Als uitgangspunt geldt het gebruik van de meest actuele versies van applicatie- en systeemsoftware; Leverancier streeft daarbij echter met name naar de optimale combinatie van de verschillende software, waarbij het kan voorkomen dat een minder actuele versie wordt gebruikt omdat deze tot een beter resultaat leidt.

9.2 Leverancier hanteert voor de bewaring van gegevens in haar systemen de wettelijke bewaartermijnen. Afnemer is zelf verplicht zorg te dragen voor de toepasselijke bewaartermijnen van de eigen gegevens.

9.3 Wanneer Afnemer het verzuimregistratiesysteem bezoekt, verzamelt Leverancier automatisch de gegevens, verzonden door computer, mobiele- of andere apparatuur waarmee men toegang heeft. Deze gegevens kunnen worden verzameld met behulp van cookies. De gebruikersgegevens die onder meer verzameld worden zijn:

- duur van uw bezoek;
- locatiegegevens op basis van uw IP-adres;
- verbindingsgegevens, zoals het IP-adres.

9.4 Om privacy de aandacht te geven die het verdient, heeft Leverancier een Functionaris Gegevensbescherming aangesteld. In geval van verdere vragen over dit onderwerp of behoefte aan meer informatie kan de Privacy Officer worden bereikt per email: [p.hendriks@verzuimondercontrole.nl](mailto:p.hendriks@verzuimondercontrole.nl).

©2020 - Verzuim Onder Controle B.V.