VRAGENLIJST PASSENDE TECHNISCHE EN ORGANISATORISCHE MAATREGELEN
Annex 2 bij het model verwerkersovereenkomst

Identificatie

Naam van de organisatie	Corilus NV / SA Gent Zuiderpoort, Atrium, Gaston Crommenlaan 4/bus 26, 9050 Gent KBO 0428.555.896
Contactgegevens	De contactgegevens van het aanspreekpunt voor informatiebeveiliging (CISO) en gegevensbescherming (DPO) kunnen geraadpleegd worden via de volgende link: https://www.corilusgdpr.com/corilus/databeveiliging en ten allen tijde opgevraagd worden via het algemeen telefoonnummer van Corilus.
Versie	v2.0 (23/04/2021)

Overzicht van maatregelen

Vraag	Enkel van toepassing indien hosting bij Corilus	Maatregel	Status
1		Beschikt u over een formeel, geactualiseerd en door de raad van bestuur goedgekeurd beleid voor informatieveiligheid?	Ja, we beschikken over een formeel beleid informatiebeveiliging en gegevensbescherming. Beide documenten worden jaarlijks tijdens een formele directiebeoordeling geactualiseerd en opnieuw bekrachtigd.
2		Heeft u een risicobeoordeling voor elk proces/project rond informatieveiligheid/gegevensbescherming die u gebruikt voor de dienstverlening?	Ja. Ondanks het toepassingsgebied van het ISO-27001 certificaat, zijn de processen rond risicobeoordeling ingevoerd voor alle teams en alle business units. Deze beoordeling behandelt zowel gegevensbescherming als informatiebeveiliging.
3		Binnen uw organisatie: Is er een dienst belast met de informatieveiligheid die onder de directe, functionele leiding staat van de raad van bestuur van de organisatie?	Ja. Wij beschikken over een Quality & Compliance team van 2 FTE die naast kwaliteit en gegevensbescherming ook actief bezig zijn met informatiebeveiliging (bv. beheer van het ISO-27001 ISMS, incidentbehandeling en opvolgen van risico's). De Quality & Compliance manager rapporteert in directe lijn aan het management team.
4		Beschikt u over een informatieveiligheidsplan goedgekeurd door de raad van bestuur?	Ja, we beschikken over een risico register waarin alle gekende risico's zijn opgenomen na identificatie, analyse en evaluatie. Ook de koppeling met behandeling (en dus passende maatregelen) is opgenomen. Maatregelen die nog niet in voege zijn worden gepland en de opvolging gebeurt via het risico register.
5		Hoeveel uren worden gepresteerd door de CISO en de DPO? •CISO (1) •DPO (2) Hoeveel uren opleidingen rond informatieveiligheid hebben de CISO en DPO gevolgd? •CISO (3) •DPO (4)	1)Minstens 120 uren / maand (behoudens ziekte, vakantie of andere afwezigheid) 2)Minstens 64 uren / maand (behoudens ziekte, vakantie of andere afwezig) 3)Minsten 40 uren / jaar 4)Minsten 40 uren / jaar Verder beschikken we ook over een Quality & Compliance team van 2 FTE. Zij beheren o.a. ook de informatiebeveiliging en gegevensbescherming en ondersteunen de CISO en DPO in hun takenpakket.
6		Neemt u de gepaste maatregelen opdat de professionele, vertrouwelijke en gevoelige gegevens opgeslagen op mobiele media enkel toegankelijk zijn voor geautoriseerde personen?	Ja. Mobiele apparaten zoals USB-sticks, cd's, dvd's en externe harde schijven mogen alleen worden gebruikt in situaties waarin netwerkverbindingen niet beschikbaar zijn of er geen andere veilige methode is om gegevens over te dragen. Bij de overdracht van gevoelige of vertrouwelijke gegevens mag volgens het beleid inzake Gegevensoverdracht alleen gebruik worden gemaakt van geautoriseerde mobiele opslagapparaten met ingeschakelde versleuteling (bv. AES-256 bit codering).

7		Treft u de gepaste maatregelen, in functie van het toegangsmedium, voor de informatieveiligheid van de toegang van buiten uw organisatie tot de professionele, vertrouwelijke en gevoelige gegevens?	Ja. Medewerkers die telewerken zijn onderhevig aan de geldende regels uit de Acceptable Use Policy, Data Classification Policy en Data Transfer Policy. Toegang tot databronnen is enkel mogelijk mits gebruik van een VPN-verbinding of mits aanmelding via Multi-Factor Authenticatie, en tevens is het niveau van aanmelding en versleuteling van de dataconnectie in relatie tot de classificatie van de databron.
8		Heeft u de telewerk-voorzieningen zo ingericht dat er op de telewerk-plek (thuis, in een satellietkantoor of in een andere locatie) geen informatie wordt opgeslagen op externe toestellen zonder versleuteling en dat mogelijke bedreigingen vanaf de telewerk-plek niet in de IT-infrastructuur terechtkomen?	Ja. Medewerkers die telewerken zijn onderhevig aan de geldende regels uit de Acceptable Use Policy, Data Classification Policy en Data Transfer Policy, welke o.a. verwijzen naar het feit dat er geen data lokaal mag worden opgeslagen en dat gegevens volgens classificatie moeten behandeld worden (bv. nooit vertrouwelijke informatie op een onbeveiligd medium).
9		Sensibiliseert u jaarlijks iedere medewerker met betrekking tot de informatieveiligheid en gegevensbescherming?	Ja. Er is een continu awareness programma met een plan per kalenderjaar dat rekening houdt met zowel gegevensbescherming als informatiebeveiliging thema's. Op jaarbasis worden er verschillende activiteiten uitgevoerd om mensen te sensibiliseren en hun te wijzen op hun verantwoordelijkheden.
10		Voert u jaarlijks een evaluatie uit rond de naleving van het beleid omtrent informatieveiligheid en gegevensbescherming in de praktijk?	Ja. Op jaarbasis worden interne audits gepland voor informatiebeveiliging en voor GDPR. Externe audits vinden plaats m.b.t. certificering zoals bv. het ISO-27001 certificaat. Verder wordt er ook geïnvesteerd in het uitvoeren van penetratietests op infrastructuur en applicaties.
11		Heeft u de toegang beveiligd door een duidelijke toegangsprocedure en heeft u een (logisch of fysiek) toegangssysteem geïmplementeerd om elke ongeoorloofde toegang te voorkomen wat betreft de gevoelige gegevens in datacenters?	Ja. Per datacenter is een procedure uitgewerkt om toegang te krijgen tot het datacenter. Onze ISO-27001 gecertificeerde datacenters staan hier ook op vermeld.
12		Heeft u de toegang beveiligd door een duidelijke toegangsprocedure en heeft u een (logisch of fysiek) toegangssysteem geïmplementeerd om elke ongeoorloofde toegang te voorkomen wat betreft de gegevens in administratieve gebouwen?	Ja. Qua logische toegang is een beleid "toegangsbeheer" ingevoerd om er o.a. voor te zorgen dat er gewerkt wordt met een access matrix, dat er scheiding van rechten plaats vindt en dat de levenscyclus van accounts structureel wordt beheerd. Qua fysieke toegang is elk van onze administratieve gebouwen uitgerust met een badge-systeem, alarm en is voorzien van een bemande receptie tijdens kantooruren. Er zijn ook beveiligingscamera's aangebracht waar nodig. Verder worden werknemers er op gewezen via de Acceptable Use Policy om geen data op te slaan op lokale media. Wat onze personeelsdienst en contract management betreft is er in het gebouw te Gent een aparte ruimte voorzien waar papier in een beveiligde ruimte wordt bijgehouden. De toegang gebeurt enkel mits toegangsbadge en is beperkt tot bevoegden.
13	**X**	Beschikt u over een classificatieschema voor persoonsgegevens waarvoor u de diensten levert en past u dit classificatieschema toe?	Ja, we beschikken over een Data Classification Policy waarin vier niveaus zijn uitgewerkt (openbaar, intern, vertrouwelijk, gevoelig). Deze worden toegepast (bv. gevoelige gegevens mogen enkel en alleen opgeslagen worden in een ISO-27001 gecertificeerd gegevenscentrum en alleen worden getransporteerd via beveiligde kanalen.
14		Heeft u de regels verwerkt in een beleid voor informatieveiligheid die gespecifieerd zijn in een beleidslijn 'email, online communicatie en internet gebruik'?	Ja, we beschikken over een Acceptable Use Policy waarin o.a. de omgang met e-mail, online communicatie en internet gebruik behandeld wordt.
15		Heeft u de regels verwerkt van het beleid voor informatieveiligheid die gespecifieerd zijn in de beleidslijn 'email, online communicatie en internet gebruik' gecommuniceerd naar alle medewerkers?	Ja, we beschikken over een Acceptable Use Policy waarin o.a. de omgang met e-mail, online communicatie en internet gebruik behandeld wordt. Hiernaar wordt verwezen via het Arbeidsreglement. Deze maken ook deel uit van onboarding van nieuwe medewerkers en periodieke sensibilisering.
16		Wanneer u 'cryptografie' wilt toepassen: • beschikt u over een formeel beleid voor het gebruik van cryptografische controles? • beschikt u over een formeel beleid voor het gebruik, bescherming en levensduur van de cryptografische sleutels voor de ganse levenscyclus?	Ja, we beschikken over een formeel en goedgekeurd beleid voor cryptografie waarin beide punten zijn opgenomen.
17		Neemt u de nodige maatregelingen ter voorkoming van verlies, schade, diefstal of compromitteren van middelen en onderbreking van de activiteiten?	Ja, we werken proactief aan preventie en bewustmaking om verlies, schade, diefstal of compromitteren te voorkomen. Los van preventie, werken we ook aan detectie (opdat we er wetenschap van zouden hebben) en een passende behandeling indien zulke gebeurtenissen zich zouden voordoen.
18		Legt u de gepaste maatregelen voor het wissen van gegevens contractueel vast met de verwerkingsverantwoordelijke?	Ja. Volgens GDPR-artikel 28 zijn klant (verwerkingsverantwoordelijke) en leverancier (verwerker) verplicht een verwerkersovereenkomst overeen te komen waarin de acties bij einde van overeenkomst worden bepaald (bv. export en/of wissen). Dit is het geval in elk van onze modellen verwerkersovereenkomsten.
19		Past u de regels toe in verband met de logging van de toegang zoals vastgelegd door de opdrachtgever?	Indien een opdrachtgever specifieke regels in verband met de logging meegeeft, dan zullen deze worden geïmplementeerd en getest zoals vooraf overeengekomen. Dit is met name zo wanneer we bv. een project opleveren.
20		Werken alle medewerkers met de ICT middelen in het kader van de diensten op basis van minimale autorisatie voor de uitvoering van hun taak?	Ja, we beschikken over een beleid toegangsbeheer waarin wordt bepaald dat rechten minimaal worden geautoriseerd en dit volgens een vooraf gedefinieerde Access Matrix.
21		Worden de vereisten voor toegangsbeveiliging (identificatie, authenticatie, autorisatie) gedefinieerd, gedocumenteerd, gevalideerd en gecommuniceerd? (1) Worden deze toegangen gelogd? (2)	1) Ja 2) Zie vraag 25

22		Voert u bij elke in productiestelling van een project een controle uit of de veiligheids- en gegevensbeschermingsvereisten die bij het begin van het project werden vastgelegd ook daadwerkelijk geïmplementeerd werden?	Ja. Om onze maturiteit nog verder te verhogen zijn we in 2021 gestart met het uitrollen van een applicatie security strategie.
23		Worden, onder de supervisie van de projectleider, de voorzieningen voor ontwikkeling, test en/of acceptatie en productie gescheiden – inclusief de bijhorende scheiding der verantwoordelijkheden in het kader van het project?	Ja. Bij al onze projecten worden de omgevingen voor ontwikkeling, test en/of acceptatie en productie van elkaar duidelijk afgescheiden.
24		Wordt elke toegang tot persoonlijke en vertrouwelijke gegevens gelogd in overeenstemming met een bedrijfspolicy omtrent “logging” en de toepasselijke wetgeving en regelgeving?	Ja. Een formele beleidslijn audit logging regelt de toegang tot persoonlijke en vertrouwelijke informatie.
25		Beantwoordt het logbeheer minimaal aan de volgende doelstellingen? • De informatie om te kunnen bepalen wie, wanneer en op welke manier toegang heeft verkregen tot welke informatie • De identificatie van de aard van de geraadpleegde informatie • De duidelijke identificatie van de persoon	Onze recente (cloud) toepassingen voldoen aan de vereiste doelstellingen. Oudere (legacy) toepassingen die niet verder ontwikkeld worden gelet op een uitfasering, hebben logging op "best effort"-wijze ingevuld.
26		Zijn de noodzakelijke tools ter beschikking om toe te laten de log gegevens uit te baten door de geautoriseerde personen (user interface of procedure)?	Indien vorig punt “ja”, hier ook “ja”. Hiermee bedoelen we: als er logs beschikbaar zijn, dan kunnen deze geraadpleegd worden binnen de toepassingen via UI, tekstbestanden of databank.
27		Worden de transactionele/functionele log gegevens bewaard overeenkomstig de Persoonsgegevens zelf (bv. 30 jaar voor medische gegevens)?	Indien vorig punt “ja”, hier ook “ja”.
28		Worden de deliverables (gegevens die verwerkt worden, de documentatie (broncode, programma’s, technische documenten, …)) van het softwareontwikkelingsproces geïntegreerd in het back-up beheersysteem?	Ja. Alle relevante artefacten uit de gehele levenscyclus van ontwikkeling zijn onderhevig aan back-upvereisten.
29		Worden, in de loop van de ontwikkeling van de Software, de behoeften met betrekking tot continuïteit van de dienstverlening geformaliseerd, conform met uw verwachtingen?	Voor onze consulting projecten nemen we voor nieuwe toepassingen steeds de nodige functionele en niet-functionele vereisten in beschouwing m.b.t. continuïteit (bv. robuustheid, redundantie, back-up, patching, procedures, …).
30	**X**	Wordt uw continuïteitsplan en de bijhorende procedures geactualiseerd in functie van de Software-evolutie, met inbegrip van continuïteitstesten?	Ons Cloud Operations ("DevOps") team heeft een formeel continuïteitsplan (incl. DRP met bijhorende procedures, DRP-testen, actieve wiki, monitoring) dat onder het toepassingsgebied van ISO-27001 valt en als dusdanig werd beoordeeld door de externe auditor. Deze zaken zijn tevens ook aanwezig bij onze datacenter providers. Voor toepassingen die niet onder de vleugels van het Cloud Operations team aangeboden worden, zijn continuïteitsprocedures ter beschikking die mee met de software en de noodzaak van klanten evolueren.
31	**X**	Wordt er een risico analyse in het begin van het softwareontwikkelingstraject gevoerd om de noodprocedures te definiëren, rekening houdend met “data protection by design”?	Ja. Ondanks het toepassingsgebied van het ISO-27001 certificaat, zijn de processen rond risicobeoordeling ingevoerd voor alle teams en alle business units. Deze beoordeling behandelt zowel gegevensbescherming als informatiebeveiliging. Rond de principes van "gegevensbescherming door ontwerp en standaardinstellingen" zijn guidelines uitgewerkt.
32		Zijn de procedures met betrekking tot het incidentbeheer geformaliseerd en gevalideerd?	Ja, we beschikken over een formele procedure voor incidentbeheer die zowel de omgang met een beveiligingslek ("security incident") als met een inbreuk m.b.t. persoonsgegevens ("datalek") behandelt.
33	**X**	Wordt de CISO op de hoogte gesteld van de veiligheidsincidenten en de DPO voor incidenten inzake gegevensbescherming?	Ja. Elk vermoedelijk beveiligingslek ("security incident") als met een inbreuk m.b.t. persoonsgegevens ("datalek") wordt gecommuniceerd naar de CISO, DPO, leden van Quality & Compliance team. Hierover wordt ook transparant gecommuniceerd met het Management Team en uiteindelijk ook aan onze Raad van Bestuur.
34		Wordt tijdens de levensloop van de Software de documentatie (technisch, procedures, handleidingen, …) actueel gehouden?	Ja. Elk ontwikkelteam heeft een documentatieplicht en zal dus o.a. technische procedures, relevante diagrammen en handleidingen maken en deze onderhouden. Veel van onze toepassingen publiceren deze ook publiek op het internet voor klanten en integratoren.
35		Worden alle middelen inclusief aangekochte of ontwikkelde systemen toegevoegd aan de inventaris van de operationele middelen? (asset management)?	Ja. Alle bedrijfsmiddelen ("assets") worden bijgehouden in een inventaris. Dit omvat o.a. alle ICT-laptops, servers, infrastructuur componenten en toepassingen.
36		Wordt de gepaste medewerking verleend aan audits uitgevoerd onder de vorm van het ter beschikking stellen van personeel, documentatie, logbeheer en andere informatie die redelijkerwijze beschikbaar is?	Ja. Volgens GDPR-artikel 28 zijn klant (verwerkingsverantwoordelijke) en leverancier (verwerker) verplicht een verwerkersovereenkomst overeen te komen waarin de mogelijkheid tot audit en onze medewerking wordt samengevat. Dit is het geval in elk van onze modellen verwerkersovereenkomsten.
37		Worden vereisten rond informatieveiligheid en gegevensbescherming gedocumenteerd om risico’s te reduceren mbt toegang informatiemiddelen?	Ja. Binnen ons ISMS en bijhorende beleidslijnen, procedures en handleidingen worden vereisten samengevat voor toepassingen met het oog op security-by-design en privacy-by-design (en default) implementatie. Elke ontwikkelde toepassing heeft use cases gedefinieerd rond beide thema's.
38		Worden alle relevante vereisten rond informatieveiligheid en privacy opgesteld en overeengekomen tussen u en derde partijen/toeleveranciers (die informatie van de organisatie lezen, verwerken, stockeren, communiceren of ICT infrastructuur-componenten en ICT diensten aanleveren)?	Ja. Met elke leverancier die optreedt als subverwerker (i.f.v. het verwerken van persoonsgegevens van onze klanten en hun patiënten / bewoners) wordt een verwerkersovereenkomst overeengekomen, waarin de relevante eisen rond informatiebeveiliging (bv. het nemen van passende maatregelen cf. GDPR-Art. 32) en gegevensbescherming (cf. GDPR-artikel 28) worden overeengekomen.

39		Wordt regelmatig de dienstverlening aan u door derde partijen / toeleverancier gemonitord, geëvalueerd en geauditeerd?	Er is een globaal contract management lifecycle proces ingericht. Hierbij worden alle leveranciers regelmatig ook gemonitord, geëvalueerd en geauditeerd o.b.v. een vragenlijst. Voor de toepassingen die onder het ISO-27001 certificaat vallen is er tevens ook een Supplier Security Policy van toepassing.
40	**X**	Wanneer u professionele, vertrouwelijke of gevoelige gegevens wenst te verwerken in een cloud voldoet u aan de minimale contractuele waarborgen?	Ja, zowel onze private cloud als eventuele cloud vendors voldoen aan contractuele waarborgen m.b.t. cloud.
41		Heeft u procedures voor het vastleggen en beheren van incidenten over informatieveiligheid of gegevensbescherming met de bijhorende verantwoordelijkheden en heeft u deze procedures intern bekend gemaakt?	Ja, we beschikken over een duidelijke incidentprocedure die rekening houdt met zowel beveiligingslekken ("security incident") als met inbreuken mb.t. persoonsgegevens ("datalek").
42		Heeft u een overeenkomst met alle medewerkers dat elke medewerker (zowel vast of tijdelijk, intern of extern) verplicht is melding te maken van ongeautoriseerde toegang, gebruik, verandering, openbaring, verlies of vernietiging van informatie en informatiesystemen?	Ja. Het arbeidsreglement werd voor intrede van GDPR bijgewerkt om de interne meldplicht van (vermoedelijke) negatieve gebeurtenissen zoals een security incident of datalek in te voeren.
43		Worden de gebeurtenissen en zwakheden over informatieveiligheid of gegevensbescherming die verband houden met informatie en informatiesystemen zodanig kenbaar gemaakt aan de opdrachtgever zodat u en de opdrachtgever tijdig en adequaat corrigerende maatregelen kunnen nemen?	Ja. Volgens de bepalingen uit de verwerkersovereenkomst en GDPR-artikel 28 in het algemeen, zijn we als verwerker verplicht om onze opdrachtgevers (in hun rol als verwerkingsverantwoordelijke) zonder onredelijke vertraging in te lichten over eventuele negatieve gebeurtenissen m.b.t. persoonsgegevens indien deze een risico zouden kunnen inhouden. Dit is mee opgenomen in ons beleid en bijhorende procedures.
44		Beschikt de leverancier over een procedure om zo snel als mogelijk intern incidenten inzake informatieveiligheid/gegevensbescherming te communiceren/rapporteren?	Ja. Volgens de bepalingen uit de verwerkersovereenkomst en GDPR-artikel 28 in het algemeen, zijn we als verwerker verplicht om onze opdrachtgevers (in hun rol als verwerkingsverantwoordelijke) zonder onredelijke vertraging in te lichten over eventuele negatieve gebeurtenissen m.b.t. persoonsgegevens indien deze een risico zouden kunnen inhouden. Dit is mee opgenomen in ons beleid en bijhorende procedures.
45		Worden bij incidenten over informatieveiligheid of gegevensbescherming het bewijsmateriaal in overeenstemming met wettelijke en regelgevende voorschriften correct verzameld?	Ja. Relevante logbestanden en eventuele elementen die als bewijs kunnen worden beschouwd worden passend verzameld en verwerkt, volgens de relevante vereisten.
46		Wordt elk incident over informatieveiligheid of gegevensbescherming formeel gevalideerd opdat procedures en controlemaatregelen verbeterd kunnen worden en worden de lessen die getrokken worden uit een incident gecommuniceerd naar uw directie voor validatie en goedkeuring van verdere acties?	Ja. Elk security incident en datalek wordt gekoppeld aan verbeteracties. We beschikken ook over een geldig ISO-27001 certificaat, waar de nadruk ligt op het aspect van continu verbetering. We integreren deze werkingen in ons DNA.
47		Brengt u regelmatig alle informatie samen om de risico's in kaart te brengen in verband met de conformiteit met GDPR en voert u de nodige acties uit als gevolg van een hoog "residueel" risico op non-conformiteit?	Ja. Elk jaar gebeurt er minstens 1x GDPR-audit en alle punten die uit zulk rapport komen worden opgepikt en gecommuniceerd aan het management team.
48		Heeft u een up-to-date centrale register van de verwerkingsverantwoordelijke of van de verwerker en heeft u een formele verantwoording voor het niet-realiseren van controlemaatregelen gericht op de naleving van de Europese verordening voor de specifieke verwerking?	Ja, we verwerken persoonsgegevens als verwerkingsverantwoordelijke (bv. rol als werkgever) en als verwerker voor onze klanten (bv. hosting, back-up, support). Voor beide rollen is een apart verwerkingsregister aangelegd, dat voldoet aan GDPR-Art. 30.