Summary of laws and regulations

The following overview contains laws and regulations that apply to [ORGANIZATION] and that may have interfaces with information security. It also keeps track of which processes it applies to, and to what extent they are complied with. This document fulfills the ISO 27001 requirement A18.1.1 (ISO 27001:2017) or A5.31 (ISO 27001:2022).

Privacy

Law/Regulation/contract	Business processes	Requirements for our ISMS	Status of implementation
General Data Protection Regulation Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG)	Almost all processes, [SECTOR SPECIFIC PROCESSES] and HR contain special categories of- and sensitive data, many supporting processes also use personal data.		Implemented. [ACTIONS TAKEN]. We have published a privacy statement: [LINK PRIVACY STATEMENT]
Telecommunicatiewet (Tw)	External websites that use cookies or other methods to track visitors.		Implemented. For example, by adding a cookie statement [LINK COOKIE STATEMENT]

Healthcare [if applicable]

Law/Regulation/contract	Business processes	Requirements for our ISMS	Status of implementation
Wet op de geneeskundige behandelingsovereenkomst (WGBO) Wet op de beroepen in de individuele gezondheidszorg (Wet	Healthcare processes	Retention period for medical information, medical confidentiality (limited sharing of information)	All of these laws are implemented and enforced. In general, this is not done by law, but with an integrated approach that has been developed to meet the

BIG) Wet kwaliteit, klachten en geschillen zorg (Wkkgz) Uitvoeringsbesluit Wkkgz Wet verplichte geestelijke gezondheidszorg (Wvggz) Wet zorg en dwang (Wzd) Wet forensische zorg (Wfz) Burgerlijk Wetboek (BW) boek 1 (m.n. bepalingen curatorschap en mentorschap) Gezondheidswet Zorgverzekeringswet (Zvw) Wet langdurige zorg (Wlz) Wet maatschappelijke ondersteuning (Wmo 2015) Jeugdwet Wet medisch-wetenschappelijk onderzoek met mensen Wet op de medische hulpmiddelen Wet op de orgaandonatie Wet publieke gezondheid Mededingingswet Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz) Wet marktordening gezondheidszorg (Wmg) Wet medezeggenschap cliënten zorginstellingen 2018 (Wmcz) Geneesmiddelenwet Wet toelating zorginstellingen (Wtzi)			requirements of Dutch law. Where necessary, advice is given by the company lawyer.

Personnel

Law/Regulation/contract	Business processes	Requirements for our ISMS	Status of implementation
Personnel law, e.g.: • Wet op de ondernemingsraden	HR-processes		Implemented. The HR department ensures the integrity, availability and

• Arbeidsovereenkomst, artikel 7:610 e.v. BW • Arbowet, -besluit en -regeling • Wet werk en zekerheid • Arbeidstijdenwet • Wet transitievergoeding arbeidsongeschikte medewerkers • Wet verbetering poortwachter • Wet DBA			reliability of personnel data. [ORGANIZATION] processes personal data when there is a legal basis for doing so. A system ([SYSTEM]) has been chosen that has been developed to comply with Dutch legislation.

Financial

Law/Regulation/contract	Business processes	Requirements for our ISMS	Status of implementation
Belastingwet	Financial processes		Implemented. The financial processes are also checked by [DEPARTMENT/ ORGANIZATION].
Archiefwet	Financial processes	Retain financial administration for 7 years	Within the financial systems, it has been ensured that the statutory retention period is observed.

Real estate [if applicable]

Law/Regulation/contract	Business processes	Requirements for our ISMS	Status of implementation
Bouwbesluiten (these contain requirements that affect continuity, for example fire detectors)	All processes that take place within [ORGANIZATION] locations		[STATUS] [EXPLANATION STATUS]

Contractual requirements

Law/Regulation/contract	Business processes	Requirements for our ISMS	Status of implementation
Arrangements with [TYPE OF SUPPLIER/THIRD PARTY]	[MAIN PROCESS]		[STATUS] [EXPLANATION STATUS]

Agreements on shared locations [if applicable]	[MAIN PROCESS] if a location (e.g. a shared restaurant/lobby) is shared with other organizations.		The [ROLE] keeps an overview of agreements and maintains contact with these organisations

ISO27001 as basis for NIS2, BIO, NEN7510

Compliance with laws and regulations from ISO 27001 standard requirement A18.1.1 (ISO 27001:2017) or A5.31 (ISO 27001:2022) is reflected in various standards that build on or are compatible with ISO27001. This makes ISO27001 a good basis for further certification and compliance with complex laws and regulations.

NIS2

The NIS2 directive (Network and Information Systems Security Directive) is intended to make the European Union safer by increasing digital protection and reducing the consequences of cyber incidents. ISO 27001 is a basis for NIS2. See https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nis2-richtlijn/

See https://regelhulpenvoorbedrijven.nl/NIS-2-NL/ whether the NIS2 applies to [ORGANISATION]:

- Does the NIS2 guideline apply to the organization?
- Is the organization Essential or Important?
- Is the organization subject to Dutch supervision?

BIO

The Bio (Baseline Informatiebeveiliging Overheid) Home NL - bio-overheid provides a joint baseline for all government organizations. The BIO describes the basic level for information security and is used within the Dutch government, by the State, Municipalities, Waterschappen, and Provinces. The BIO has the same structure as ISO 27001 but has further elaborated the control measures.

NEN7510

NEN7510 is about information security in healthcare https://www.nen.nl/zorg-welzijn/ict-in-de-zorg/informatiebeveiliging-in-de-zorg. Since 2008, the law states that healthcare providers must comply with NEN 7510. This follows from the Additional Provisions for the Processing of Personal Data in Healthcare Act (Wabvpz). NEN7510 adopts 93 management measures from ISO 27001 and has approximately 10 additional healthcare-specific measures.

Intellectual property

Applicable laws and Regulations:

- Auteurswet (Aw)

[ORGANIZATION] prefers purchasing standard software packages to custom solutions. The regular procurement process is followed to ensure compliance with legal, regulatory and contractual requirements related to intellectual property rights and the use of proprietary software products. Contractual terms and conditions govern the handling of intellectual property.