1. Document details

1.1 Document properties

Document property	
Title	
Subject	
Author	
Document type	
Version number	
Classification	
Date	
Owner	
Approved by	
Date of approval	
Status	

1.2 Version management

Version management

Version	Date	Author	Changes

DIA-SOLUTIONS
SOFTWARE FOR HEALTHCARE

Content

2. Inleiding

2.1 Purpose of the document

2.2 Scope

3. Short description

LEGISLATION[2]	SHORT DESCRIPTION AND EXPLANATION APPLICABILITY FOR DIA-SOLUTIONS	URL	INFORMATION SECURITY	PRIVACY
General data protection regulation (GDPR) (Uitvoerings wet Algemene Verordening Gegevensbescherming (UAVG))	**Brief description:** Regulation on the protection of natural persons regarding the processing of personal data and the free movement of such data. The GDPR is directly applicable in Europe. Where the GDPR leaves room for choice in the implementation of the GDPR, the Netherlands has laid down rules in the Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG). **Explanation of applicability for DIA-Solutions:** The entire regulation applies because personal data are processed within DIA-Solutions.	https://eur-lex.europa.eu/legal-content/NL/ALL/?uri=CELEX:32016R0679 https://wetten.overheid.nl/BWBR0040940	•	•
Algemene wet bestuursrecht (Awb)	**Brief description:** General rules on the relationship between government and citizens. This includes administrative procedural law. **Explanation of applicability for DIA-Solutions:** In principle, the Awb does not apply to DIA-Solutions, as it is aimed at administrative bodies. However, Articles 5.16 and 5.17 may entail powers that affect DIA-Solutions. For example: power to demand information, or to demand business data and documents.	https://wetten.overheid.nl/BWBR0005537	•	•
Algemene wet inzake rijksbelastingen (AWR)	**Brief description:** General law regulating a number of taxes. **Explanation of applicability for DIA-Solutions:** Everyone is obliged, if requested, to provide the inspector with the data and information that may be relevant for the taxation (article 47 AWR). For a refusal to comply with the tax assessment obligations of third parties, DIA-Solutions cannot invoke the circumstance that they are bound to secrecy by virtue of	https://wetten.overheid.nl/BWBR0002320	•	•

	their profession (section 53a AWR). The general retention obligation of data carriers is seven years (Section 52 AWR).			
Arbeidsomstandighedenwet	**Brief description:** Provisions to improve working conditions. This Act is addressed to all labour organisations in the Netherlands. The starting point of the Arbeidsomstandigheden, is that conducting a policy on working conditions is the responsibility of the employer in cooperation with the employees, with expert support where necessary. **Explanation of applicability for DIA-Solutions:** The employer shall immediately report occupational accidents resulting in death, permanent injury or hospitalisation to the designated supervisor and shall report to this supervisor as soon as possible upon request. The employer shall keep a list of the reported occupational accidents and of occupational accidents that resulted in an absence of more than three working days and shall record the nature and date of the accident. (Art. 9 paragraphs 1 and 2)	https://wetten.overheid.nl/BWBR0010346		•
eIDAS regulation	**Brief description:** Regulation on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC **Explanation of applicability for DIA-Solutions:** The tokens of the digital signature must comply with the level of reliability set out in the regulation, see Article 26 of the regulation. The electronic signature must be used only under the sole control of the signatory. Qualified means for creating electronic signatures must meet the requirements of Annex II of the Regulation, including the level of security. DIA-Solutions itself therefore does not have to meet those security requirements, but the means used does.	https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32014R0910	•	•
Grondwet (Gw)	**Brief description:** The Grondwet (Constitution) is the most important state document and supreme national law of the Netherlands. It contains the rules for our state structure and the fundamental rights of citizens. **Explanation of applicability for DIA-Solutions:** Article 10 GW: paragraph 1 everyone has, subject to limitations to be imposed by or pursuant to the law, the right to respect for his privacy. Paragraphs 2 and 3 state that the law must lay down rules to this end. Paragraph 1 addresses DIA-Solutions in this sense because DIA-Solutions must safeguard this privacy and the rights of the data subjects and has to take this into account by implementing information security and safety requirements. These include:	https://wetten.overheid.nl/BWBR0001840	•	•

	- The right to freedom of expression (Article 7); - The right to respect for privacy (Article 10); - The right to confidential communication (Article 13).			
Handelsregister besluit	**Brief description:** In particular, the Handelsregisterbesluit contains obligations regarding registration in the commercial register at the Chamber of Commerce (CoC) ("Kamer van Koophandel"). **Explanation of applicability for DIA-Solutions:** The register may include data on proxies of a legal entity. In that case, their personal data and the contents of their power of attorney are recorded. It also includes personal data on 'every director and supervisory director' of a private or public limited company (NV/BV). (The decree addresses the question: what to register in?) Relevant articles: Art.12, 13, 14, 17, 18, 22, 30	https://wetten.overheid.nl/BWBR0028479		•
Commercial Register Act (Handelsregisterwet (Hrw))	**Brief description:** This law contains provisions on mandatory registration in the commercial register ("handelsregister") at the Chambers of Commerce ("Kamer van Koophandel"). **Explanation of applicability for DIA-Solutions:** Submitting statements via Digipoort to the Chamber of Commerce. The Commercial Register Act requires companies to register with both the Chamber of Commerce of the area where the company itself is established and with all Chambers in the area where they have a branch office. Background to this is the desirability of having the relevant details of business activities in the region at each Chamber of Commerce.	https://wetten.overheid.nl/BWBR0021777	•	•
Dutch Telecommunication Act (Telecommunicatiewet (Tw)	**Brief description:** This sets out the main rules that providers of an electronic communications network must comply with. **Explanation of applicability for DIA-Solutions:** On 1 July 2021, the Telecommunications Act changed. Main changes: 1. You may only approach potential customers with opt-in. Cold acquisition is still allowed towards corporate legal entities if those details have been disclosed for that purpose. 2. You may call customers for similar products or services, as long as the right to object is offered. 3. The do not call me register disappears. No more default opt-in until opt-out. 4. Telemarketing with an anonymous number is prohibited. 5. Tracking of opt-ins is mandatory.	https://wetten.overheid.nl/BWBR0009950	•	•

	The Telecommunications Act defines consent as free, specific, informed and unambiguous expression of will. By which the data subject accepts, through a statement or unambiguous active action, the processing of his data. As an organisation, you must be able to prove consent obtained. Withdrawing consent must be as simple as giving it. There should be no adverse consequences for the person withdrawing consent.			
Anti-Money Laundering and Anti-Terrorist Financing Act (Wet ter voorkoming van witwassen en financieren van terrorisme)	**Privacy** This law is a merger of the Wet identificatie bij dienstverlening and the Wet melding ongebruikelijke transacties, aimed at preventing the use of the financial system for money laundering and terrorist financing. **Explanation of applicability for DIA-Solutions:** Retention of supporting documents: retention periods and system requirements (art.33).	https://wetten.overheid.nl/BWBR0024282	•	•

Dutch Criminal Code
 	
(Wetboek van Strafrecht)
	Brief description:
	The Dutch Criminal Code regulates which offences are considered felonies and which offences are considered misdemeanours, and the types of penalties that can be imposed for them.
	
	Explanation of applicability for DIA-Solutions:
	Employees could misuse the ICT facilities made available to them. Monitoring of employees by DIA-Solutions to identify misuse is in principle lawful, but there is also the right to privacy in the workplace. A monitoring policy should be announced and be as specific as possible. The Works Council must give its consent, as monitoring falls under a personnel monitoring system (Art. 27 WOR).
	
	The Dutch computer crime Act II and III (wetsvoorstel computercriminaliteit) amended or introduced several provisions in the Criminal Code. The offences in question are crimes:
	• Against data availability:
	  ○ Hacking, virus/malware, sniffing (Art. 138a Sr);
	  ○ Spamming, virus/malware (Art. 161 sexies Sr);
	  ○ Web defacing, Denial of Service (Art. 138a, 350a, 350b, 161sexies-septies SR);
	  ○ Data damage, virus/malware (Art 350a Sr).
	• Against data confidentiality:
	  ○ Eavesdropping and wiretapping, sniffing (Art 139a-e, 441a Sr);
	  ○ Trade secrets (Art 273 Sr).
		https://wetten.overheid.nl/BWBR0001854	•	•

4. Specifically applicable laws and regulations for healthcare

4.1 Dutch legislation

LEGISLATION[3]	SHORT DESCRIPTION AND EXPLANATION APPLICABILITY FOR DIA-SOLUTIONS	URL	INFORMATION SECURITY	PRIVACY
Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz)	**Brief description:** The purpose of this law is to create additional framework conditions for the use of an electronic exchange system by healthcare providers in order to protect client privacy. **Explanation of applicability for DIA-Solutions:** Key provisions: • The client has the right to consent to data being accessed or made available through an electronic exchange system; • Certain categories of healthcare providers should be able to be excluded from this consent; • The client must be able to inspect the file or receive a copy of the file upon request; • The client has the right to see who has made certain information available or consulted it (logging obligation NEN7513); • The client must be informed about how the client can exercise his/her rights; • A prohibition for health insurers, company and insurance doctors to access electronic exchange systems.	https://wetten.overheid.nl/BWBR0023864	•	•
Wettelijk voor geschreven bewaartermijnen	**Brief description:** The GDPR states that personal data should not be kept longer than necessary and does not propose concrete retention periods. However, there are concrete retention periods that organisations must adhere to. For example, under tax laws. **Explanation of applicability for DIA-Solutions:** Retention periods and their justification should be laid down in the privacy policy or a retention policy.	https://autoriteitpersoonsgegevens.nl/nl/over-privacy/persoonsgegevens/bewaren-van-persoonsgegevens	•	•

4.2 Field standards[4]

LEGISLATION	SHORT DESCRIPTION AND EXPLANATION APPLICABILITY FOR DIA-SOLUTIONS	URL	INFORMATION SECURITY	PRIVACY
Gedragscode Elektronische Gegevensuitwisseling in de Zorg (EGiZ)	**Brief description:** The electronic exchange of personal data must comply with European and national legal requirements. The Gedragscode Elektronische Gegevensuitwisseling in de Zorg (EGiZ) (a Code of Conduct on Electronic Data Exchange in Healthcare) provides practical guidelines for healthcare providers and partnerships to comply with applicable regulations. **Explanation of applicability for DIA-Solutions:** Key obligations from the EGiZ gedragscode: • Personal data may only be exchanged when necessary for the proper treatment of the client. • The client has the right to be informed about data processing and the right to give (and withdraw) consent when data is exchanged. • The responsible party (DIA-Solutions) should establish and publish an authorisation policy. • The treatment relationship should be established and tested. • The exchange of personal data should be adequately secured. • Actions should be logged.	https://www.knmg.nl/actueel/publicaties/elektronische-gegevensuitwisseling-egiz	•	•
Wet elektronische gegevensuitwisseling in de zorg (Wegiz)	**Brief description:** The Wet elektronische gegevensuitwisseling in de zorg (Wegiz) (an Electronic Data Interchange in Healthcare Act) is a framework act with supplementary rules specifying which data exchanges, and from when, must take place electronically. The act stipulates not only that healthcare providers must exchange data with each other electronically (track 1), but also according to which agreements this must take place (track 2). **Explanation of applicability for DIA-Solutions:** The Wegiz requires healthcare providers to exchange medical data electronically, making information about a patient's treatment and care more readily available and reducing the risk of errors.	https://www.gegevensuitwisselingindezorg.nl/wegiz/uitleg-over-de-wet	•	•

NEN7510 (information security in healthcare)	**Brief description:** NEN7510 is the standard for organising and securing information security in healthcare. The standard is aimed at all small and large organisations dealing with this. NEN7510 is a general standard for information security. NEN7512 and NEN7513 elaborate on this standard for a specific focus area. **Explanation of applicability for DIA-Solutions:** Key commitments: • Establish and control an ISMS (Information Security Management System) with a PDCA (Plan Do Check Act) cycle; • Conduct risk analyses and manage risks adequately; • Ensure continuous employee awareness; • Learning from incidents to prevent recurrence.	https://www.nen.nl/nen-7510-1-2017-a1-2020-nl-267179	•	•
NEN7512 (basis of trust for data exchange)	**Brief description:** NEN7512 aims to provide assurance to parties exchanging medical data between themselves. NEN712 complements NEN7510 for risk classification and elaboration of requirements on identification and authentication associated with a risk class. An example is sending a client transfer message.	https://www.nen.nl/nen-7512-2022-nl-297137	•	•
NEN7513 (recording actions in electronic patient records)	**Brief description:** NEN7513 sets requirements for healthcare providers' access logging to electronic client records. All actions of healthcare providers must be logged in a system to check the legitimacy of access to the client file. This makes the standard an applicable and uniform interpretation of existing legislation, in particular the WGBO (treatment relationship and professional secrecy). **Explanation of applicability for DIA-Solutions:** NEN7513 provides healthcare providers with frameworks for logging and using this logging to comply with legal obligations. The NEN7513 also sets requirements for the record systems used. These requirements are particularly important for software suppliers. The standard stipulates that clients or an (internal) supervisor must be able to request the logging, for instance in case of suspected abuse. Key provisions: • Important events must be recorded; • Important events are, for example: accessing, mutating and deleting, using the 'emergency procedure' and creating or modifying authorisations; • It must be recorded who performed the action, which client and/or what data it concerned.	https://www.nen.nl/artnr/309856	•	•

5. Managing compliance and deviations

5.1 Security incidents

5.2 Exceptions

5.3 Sanctions and consequences of violations

5.4 Audit and compliance checks

5.5 Periodic assessment and review of policies