Castor Assessment of GDPR and HIPAA Compliance

GDPR Compliance	Relevant articles of the GDPR	Implementation
Territorial Scope	**Article 3**	Customers have the option of hosting data in Data Centers located in The Netherlands, US, UK or Australia. For European trials, this means that medical data will not be transferred outside of the EU.
Principles relating to processing of personal data. **Employee awareness training**	**Article 5**	Personal data of Castor Employees is collected solely to support their work at Castor. For Customers, personal data is collected solely to support and improve their interactions with Castor. This primarily requires each contact's full name, username, title/role, email address, phone number and job responsibilities. For Patients, the entry and use of personal data is the responsibility of the Customer. Castor provides secure hosting of the applications and corresponding databases. Only limited personnel within Castor have access to production databases based on their role. Authorizations are granted on the 'need to know' and 'least privilege' principles. These access restrictions are described in SOPs. All employees are aware of commitment to protecting patient information and are properly trained in Data Privacy, GDPR, and HIPAA.
Lawfulness of processing	**Article 6**	Castor performs no processing of personal data other than is necessary to manage its Employees, support its Customers, respond to prospective Customers and fulfil its obligations to manage clinical trial data based on contractual requirements with Customers.
Conditions applicable to child's consent	**Article 8**	Castor assumes that, for Patients in pediatric trials, informed consent is signed by the child's authorized representative. Therefore no additional provisions are required for a child's consent. Ultimately, this is the responsibility of the Customer.
Processing of special categories of personal data	**Article 9**	No such personal data is collected directly from Customers by Castor. For Patients, where medical, genetic or biometric data can be collected, Castor assumes condition 2(a) of Article 9 applies. i.e., the patient has given explicit informed consent. Data is protected using technical and organisational security measures.
Privacy Statement	**Article 5, 12, 13, 14, 15,**	By visiting Castor's websites and by using its services, website visitors and Customers are trusting Castor with their personal data. In the privacy and cookie statement Castor explains which data it collects and for which purposes. See Castor Privacy and Cookie Statement.

Data Portability	**Article 20**	Participants of investigational studies must request data through Investigator, Sponsor, or CRO. Data Controller will contact Castor with any requests. Castor has a documented procedure in place to carefully handle these specific requests. Our "Data Subject Request Procedure" describes this process. It can be reviewed during audits.
Data Retention Policy	**Article 5, 13, 17 and 30**	Castor documents its data retention policy in a processing activities registry according to article 30 GDPR. Castor's "Document management and retention policy" can be reviewed during audits.
Security of processing	**Article 5, 18, 32**	Integrity and honesty are the key attributes of everything we do at Castor. We are committed to protecting our customers' data above all else. Castor is secured according to the most recent standards in order to protect your data in the best possible way. See Castor Security Statement.
Appointment of DPO	**Article 37-39**	Castor has appointed an external DPO in order to comply with the obligations under the GDPR.
Data Subject Rights Policy	**Article 15-23**	Castor has a documented procedure in place to carefully handle these specific requests. Our "Data Subject Request Procedure" describes this process. It can be reviewed during audits.
Responsibility of the Controller	**Article 24,28**	Castor is the controller of Employee data; and the processor of Patient data. Appropriate SOPs and security measures have been put in place to ensure correct organizational processes are followed when collecting and handling personal data. Security measures and the associated tools for managing security are outlined in more detail in Castor's "Information Security Policy", which can be accessed during audits. General Information disclosed in Castor Security Statement.
Privacy by design and by default	**Article 25**	"Secure Development & Quality Assurance Policy" and "Security/Privacy by Design Checklist" describe how these measures are implemented. Authorizations to internal environments and systems are granted on the 'need to know' and 'least privilege' principles.
Data Processing Agreement (Castor customers) Engaging Sub Processors	**Article 28**	Castor's obligations towards its Customers is covered under the Master Service Agreement "MSA Ciwit B.V". Castor also maintains a Supplier procedure that includes the completion of a DPA.
Data Processing Agreement (Suppliers - Castor as Controller)	**Article 24 and 28**	Castor has a specific procedure in place to make sure products and services are purchased with suppliers who comply with Castor's selection criteria and are onboarded according to Castor requirements (including the correct documentation), both to make sure all purchased products and services comply with the quality and information security standards needed for Castor.All details are covered under Data Processing Agreements.
Data Processing Agreement (Suppliers - Castor as Sub-Processor)	**Article 28**	Castor has a specific procedure in place to make sure products and services are purchased with suppliers who comply with Castor's selection criteria and are onboarded according to Castor requirements (including the correct documentation), both to make sure all purchased products

		and services comply with the quality and information security standards needed for Castor. Covered under Data Processing Agreement.
Records of processing activities	**Article 30**	Documented in "Castor GDPR - Processing Activity Register" For Patients, the sponsor or CRO is responsible for the obligations set out in paragraph 1 of Article 30 as the controller. For Castor Customers, under paragraph 2, Castor only performs processing based on a signed Work Order or Change Request as the processor. MSA's and DPA's include details of processing activities and sub-processors.
Data breach procedure	**Article 28, 33 and 34**	If a data breach poses a risk to an individual's rights and freedoms, Castor has a "Personal Data Breach management procedure" in place to notify the supervisory authority without undue delay, and at the latest within 72 hours after having become aware of the breach. If Castor operates as a data processor it will notify every data breach to its Customer(s) within 48 hours.
Cooperation with the supervisory authority	**Article 31**	Castor has an established process for supporting a regulatory inspection.
Records of (possible) data breaches	**Article 33**	Castor has an overview of all (possible) security incidents and data breaches, managed through a CAPA List in Legisway
Privacy Impact Assessment	**Article 35**	A Data Protection Impact Assessment (DPIA) is a process that helps Castor identify and minimise the data protection risks of a particular service or product. Castor will perform a DPIA if type of processing is likely to result in a high risk to individuals.
Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.	**Article 89**	General information disclosed in Castor Security Statement

Castor HIPAA Compliance

Castor ensure compliance with HIPAA requirements through:

- ✓ Awareness Training to all employees
- ✓ Establishment of data and privacy policies and procedures, including Data Breach Policy
- ✓ Risk Analysis and Management to track access of PHI
- ✓ Administrative Safeguards: Security Management, Security Training, Information Access Management
- ✓ Technical safeguards to protect access to data
- ✓ Data Integrity Controls
- ✓ Periodic reviews and Internal Audits to evaluate the effectiveness of security measures
- ✓ Establishment of Privacy Officer