Pridatect

WEBINAR

Health Apps and Data Protection

Lisa Hofmann

Chief of Legal Operations
Pridatect

Legal specialist and certified Data Protection Officer, broad experience in helping companies with their privacy compliance

Charles Maddy-Trevitt

GDPR Compliance Lead

UK Market GDPR Specialist Background in a wide range of industries/sectors with international experience (US/UK/Canada/EU) in data protection

We want to hear from you!

Send your questions to:

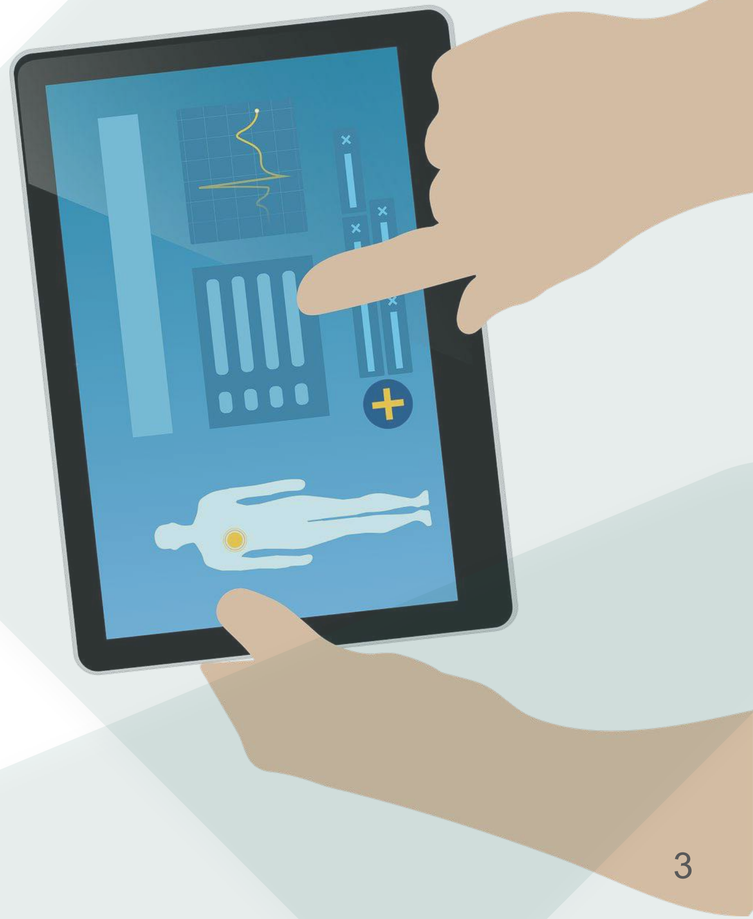
lisa.hofmann@pridatect.com

Digital applications in the health industry

The market for health apps is booming: apps for health monitoring, making a diagnosis, therapy, or even use digital resources to solve health problems.

GDPR categorises data relating to people's health as particularly sensitive, so all the necessary measures must be taken to protect their safety.

The Covid-19 pandemic has led to a huge increase in the number of apps that deal with health-related data.



Data protection regulations applicable to health apps

Charter of Fundamental Rights of the European Union (Art. 8)

General Data Protection Regulations.

Common Law Duty on Confidentiality & NHS Act 2006 approval

DPA 2018 provides the basic regulation of patient rights and obligations regarding clinical information and documentation.

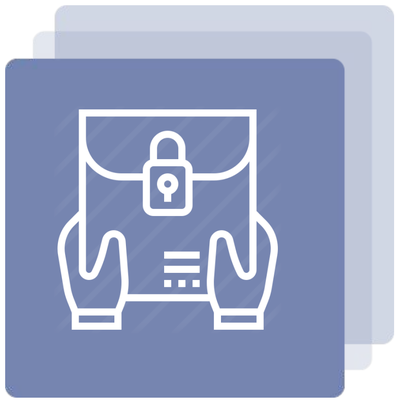
Privacy issues with health apps

Some digital products, such as fitness or health apps, collect personal health data that is sensitive and therefore needs special protection

What are the health apps?

Principles of data protection

Examples of apps



Legal basis for the processing of health data

The processing of health data is prohibited according to Art. 9 para. 1 GDPR, unless one or more exceptions from Art. 9 para. 2 GDPR apply

- Consent, Art. 6 para. 1 lit. a, Art. 9 para. 2 lit. a GDPR
- Preventative Health Care, Art. 9 para. 2 lit. h GDPR
- Cross-Border Threats to Health, Art. 9 para. 2 lit. i GDPR

"Depending on the legal basis, there are also different requirements for the provider.

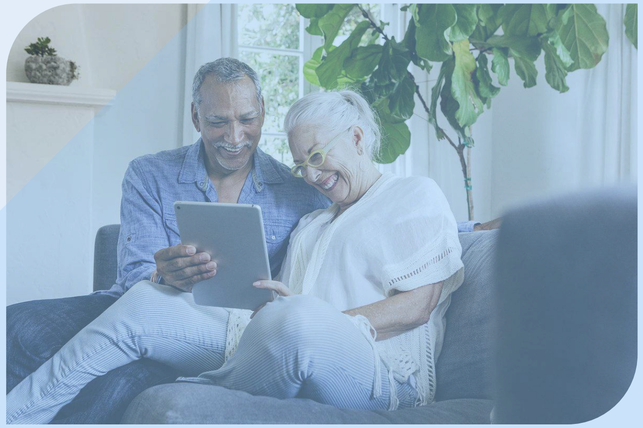
Bases of legitimacy for the processing of health data

Consent for the processing of health data can be considered to have been given under any of the following conditions:

- If clear, firm and specific consent has been given voluntarily
- Consent can be given in writing or electronically
- The information has been given in a sufficiently clear and inclusive manner:
  - Who is the data controller
  - What data will be processed
  - Purpose of data processing (separate consent must be given if there are different processing purposes).
  - Whether the data will be shared or processed with or by third parties.
  - The right for the data subject to withdraw his/her consent at any time.
  - This information must be given in an understandable form, with clear and simple language.

Consent for minors: the consent of the legal guardian would be required

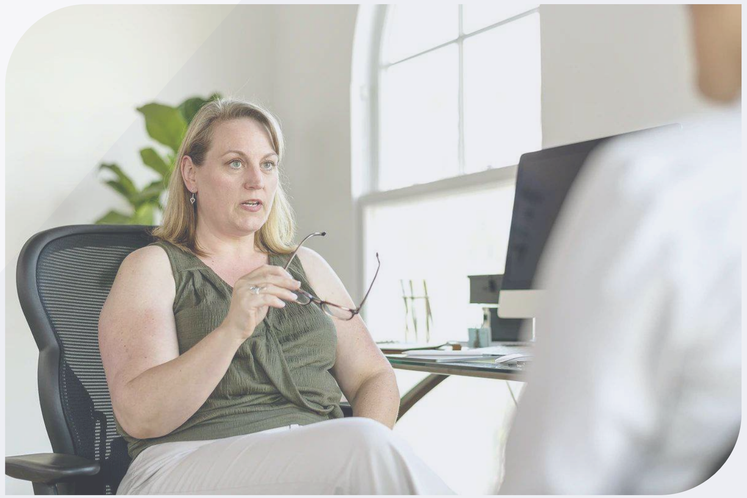
"It is important to have a statement that clearly demonstrates consent"



Good practices for companies developing health apps

Aspects to be taken into account, from the point of view of data protection, in the development of health apps by the Data Controller

- Write legal notices and privacy policies that indicate the treatment of data in a clear, simple and understandable way.
- Carry out an Impact Assessment.
- Appoint a Data Protection Officer.
- Make an exhaustive list of those responsible for the treatment.
- Carry out secure data protection policies (data retention, etc.)
- Be able to demonstrate consent.
- Minimization of data
- Anonymize data.
- Registry of Processing Activities & Processing



Safety measures in applications

Data protection can be better controlled in data processing operations if it is already technically integrated when the applications themselves are developed

Privacy by design
= Data protection through technological design

It is carried out through the early adoption of technical and organisational measures (TOMs) in the development stages

Default Privacy
= Data protection through user-friendly default settings

The application settings must already be created in a data protection-friendly way

Specific services for companies in the health sector

- Appointment of a **Data Protection Officer (DPO)** Every company in the health sector needs to appoint a DPO. Pridatect offers the service of external DPO for all those companies that do not have one.

- **Impact Assessment** When dealing with sensitive data it is mandatory to perform PIAS. Pridatect facilitates the implementation of PIAS for each Treatment Activity Record (TAR) carried out by the company.

- **HIPAA compliance** With Pridatect, all companies operating in the US will be able to comply with the US physician services standard.

"Pridatect provided us with an expert team who have been unwaveringly helpful.

Working with Pridatect has taken much of the pressure off of the Co-Founders so we can focus on supporting vulnerable individuals."

Hector Alexander
COO & Co-Founder of Yokeru
Technology to monitor the health of the most vulnerable in our society

Pridatect, a platform to simplify the process of identifying risks and protecting data

DETECT AND IDENTIFY RISKS

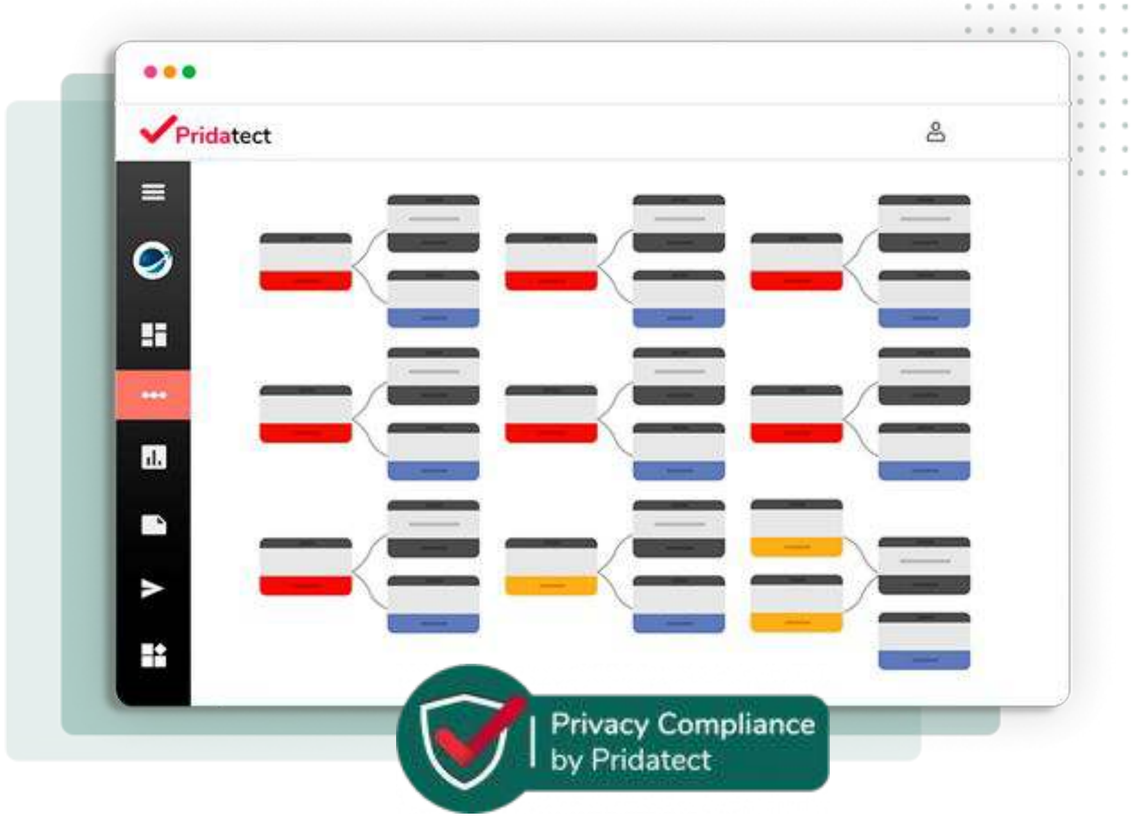
Detect and identify risks in your personal data processing (customers, employees, suppliers...). With the Pridatect platform we can identify and analyse the threats and vulnerabilities in your processes.

DEFINE AND SUGGEST MEASURES

Knowledge of the risks in your company allows us to define the necessary measures to reduce and mitigate them. Pridatect helps you with the definition and suggestions of measures for your company.

PROGRAMME MONITORING AND IMPLEMENTATION

Data protection is an on-going task within a company. Pridatect not only helps with the initial implementation, but also with the continuous monitoring of risks, measures and task management among your company's employees.



Trusted technology solution for your data protection

Everything you need to comply with GDPR

Risk assessment

Eliminate data risks

Impact assessment

Automated impact assessment

Compliance analysis

Identify gaps in your data protection

Processing Activities

Have an up-to-date record of processing activities

Data map

Map your company's data flows

TOMs

Defines technical and organizational measures to reduce risk

Privacy reports

Generates privacy reports automatically

International transfers

Manages international data transfers

Security Gap Management

Successfully handles security breaches

Fulfillment of your website

Generates privacy policies, cookie policies, terms and conditions

Subject access rights

Manages requests for access rights and subjects

Secure Userdesk Cloud

100% secure, collaborative cloud environment

External DPO service

Virtual DPO for your company

Contracts with suppliers

Generate the contracts you need for GDPR

Document Automation

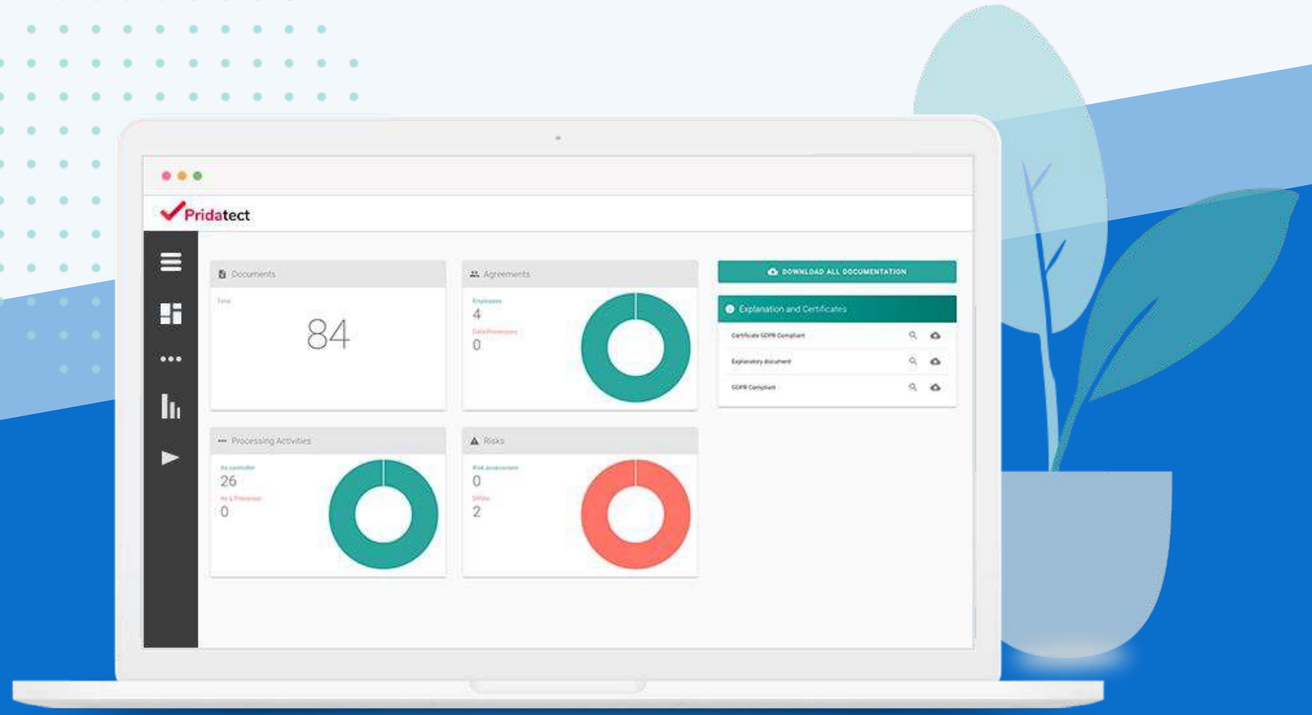
Create legal documents based on our models

Try Pridatect!

Take control of data protection management and ensure that everyone in your company has the necessary guidelines to prevent putting putting data at risk when teleworking. At Pridatect we help you to detect risks and take the appropriate measures.

Contact us for a free demo or use our 7-day free trial.

Request your free demo



Thanks for joining our **Webinar!**