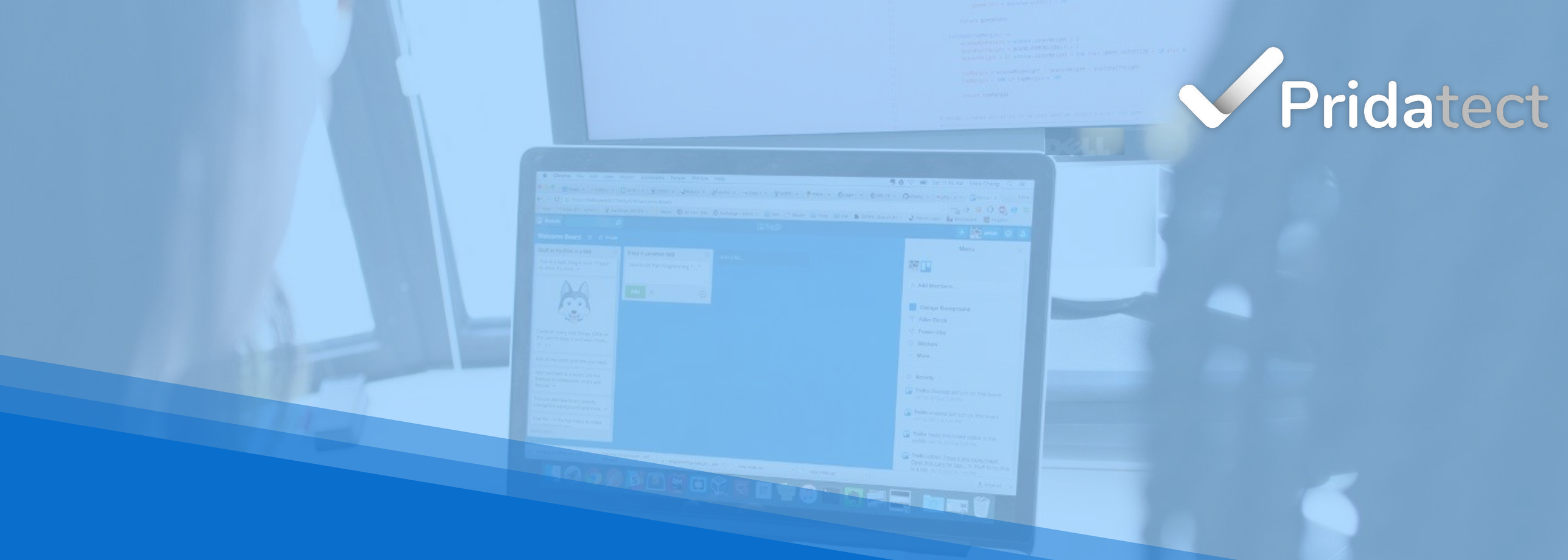


Pridatect

WEBINAR

Online Education 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

Ben Seretny

Data Protection Officer
DPO Centre

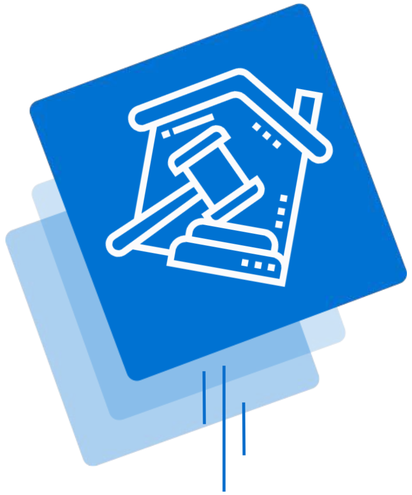
Certified Information Privacy Manager with a strong background in the pharmaceutical, healthcare and legal sectors.

Send us your questions!

lisa.hofmann@pridatect.com

Contents

Introduction



Applicable regulations

Processing data of educational centres on the Internet

How to choose a platform that guarantees security?

01. Introduction

The suspension of normal education provision in accordance with the Government's Health Protection Regulations has meant that schools have moved towards **delivering online education** and the use of different technologies in a hurry.

Special attention must be paid to the protection of personal data, such as the **image and voice of students and staff, as well as the processing of other personal data such as name, surname, age, academic background, etc.**

The non-consensual dissemination of academic activity outside the framework of the subject itself may violate the **fundamental rights to data protection.**

02. Applicable regulations and governance

Carrying out educational activities means you need to process personal data of children, as well as of other groups such as teachers and parents, who are going to be present at different times, so it is necessary to know how the regulation of this fundamental right to data protection and respect for privacy is applied, paying special attention to the protection of children.

GDPR AND DPA 2018:
Obligation to designate a DPO

Article 50 TEU:
Despite the UK's exit from the EU on 31st January 2020, the GDPR will continue to have full effect within the UK throughout the transition period until 31st December 2020.

ICO adjustments to regulatory approach: will be "empathetic and pragmatic" during pandemic.

Accountability still remains at the forefront of all processing activities

If you are interested to learn more on the topic watch our webinar: GDPR after Brexit

Personal data and sensitive data

There is certain data, such as that relating to children, that because of its relevance and importance to privacy must be treated and stored with greater care and in compliance with a series of requirements. Not all personal data is of equal importance.

What is "personal data", according to the GDPR?

- Identifiable information such as first name, last name, telephone number, etc.
- Pseudonymized data or non-direct identification information, which does not allow the direct identification of users but does allow individualized behavior.

What is sensitive data?

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Union membership
- Genetic data
- Biometric data in order to uniquely identify an individual
- Those data relating to health or sex life and/or sexual orientation

Do you really need to use that personal data?

- Many online learning resources can be downloaded or accessed without the the requirement for registration or the use of personal data.
- The Department for Education has provided a list of approved remote education tools which can be utilised without the need for additional processing of personal data
- Resources such as Oak National Academy have been developed by educational professionals during the pandemic to facilitate online learning and to support teachers and students during the lockdown.

03. Processing data of educational centres on the Internet

Educational platforms

- The educational centres **are responsible for the processing** as soon as they acquire the services of the respective platforms.
- The processing of the data by the educational centres is covered by state and autonomous community legislation and the consequent legal relations that derive from it.
- Tools other than educational platforms may also be used.

"Schools must inform parents about the use of new educational platforms, technologies or Apps, as long as they treat their personal data".

What are the risks associated with e-learning?

A **Data Protection Impact Assessment** will provide a framework to identify and minimise/remove risks

These may be mandatory when engaging a new online e-learning provider.

Regardless of when the processor was engaged, the risks should be assessed. The current situation may have changed the risk profile of a previously established method of remote teaching.

Think About:
Purpose - inside the scope of education provision?
Lawful basis - will special categories of data be involved?
Data subject rights - can you guarantee them?
Minimisation and limitation - can settings be limited?

How to screen potential solutions & lawful basis for use

Distributed processor engagement can lead to failures in due diligence and monitoring. Allowing department heads to select products on features alone can create **multiple risk factors for data subjects** using the service

Build a **protocol/ policy for screening and engaging** e-learning services to prevent supplier products slipping through the cracks.

Developing or leveraging an existing **Information Governance team** will aid compliant contracting and reduce the appearance of risks when selecting vendors.

Identify the correct lawful basis - is the service integral to the provision of education?
If special categories of data will be processed (for counselling and similar activities), what will the appropriate lawful basis be?

What is an acceptable use for non-educational platforms?

- The recent transition to remote provision of education has lead to **a rise of non-EdTech products**, which can create further risk factors for education centres.

- Regardless of the popularity of the platform, you should **assess the suitability** of each. Can safeguarding standards be ensured?

- The “user risk” is greater in **uncontrolled environments** such as general purpose video conferencing tools. Once gain, consider “is it the best medium” and “is it required” with other tools available?

- **Teachers should be educated** on delivering classes remotely and a code of conduct should be adapted for online provision of lessons, much the same as would be in place normally.

- If using a general access platform (YouTube, etc) consider restricting the access, try to avoid any identification of students by way of reference and always assess the necessity of using recorded mediums for teaching.

Key considerations during lockdown

Work with your vendors & work with your audience: Choosing a product which suits your requirements and framework as well as the resources of your audience is key. And keep students and parents informed of any changes in software usage.

Educate your users - implement policies or guidelines for safe use. Think about conduct as much as security.

Update your records of processing - consider a separate "Lockdown RoPA" if processing begins to deviate greatly from the norm.

Notify your data subjects on how their data will be used. Privacy notices need to be accurate and reflect any novel usage of personal data during the lockdown period.

Publication of images of children on websites and social networks

- They may be published **when consent is given** or students cannot be identified.
- Correct policies should be in place to govern the collection of consent, storing, publication, suitability and removal of any photos taken for media purposes.
- *Similar measures should be in place to request consent for the publication of parent/carer photos as well.*

"It is necessary to inform about the data to be published, on which social networks, for what purpose, who can access the data, and the rights of access, rectification, opposition and deletion".

04. How to choose a platform that guarantees privacy?

In certain cases, in order to carry out their functions, educational centres need the collaboration of software external to the centre that is necessary to carry out the services.

Consider how suitable the software will be for all stakeholders - does it align with your existing privacy framework and your student's access to hardware.

We recommend reading the information about the service (privacy policy and terms of use) before you start using it

When contracting cloud computing services, international data transfers can be made if the servers are outside the EEA. In any case, the requirements established by the regulations must be complied with.

Choose a vendor that works with you to ensure data protection standards are met. Do they have their own DPIAs, security assurances, adequate DPAs.

When providing data in any area (in any type of application, in the registration of users, in the contents) avoid incorporating data of the domicile of the children and other personal data that could endanger their security.

Restricting access permissions
Data Encryption
Secure networks
Metadata
Secure deletion

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

DETECT AND IDENTIFY RISKS

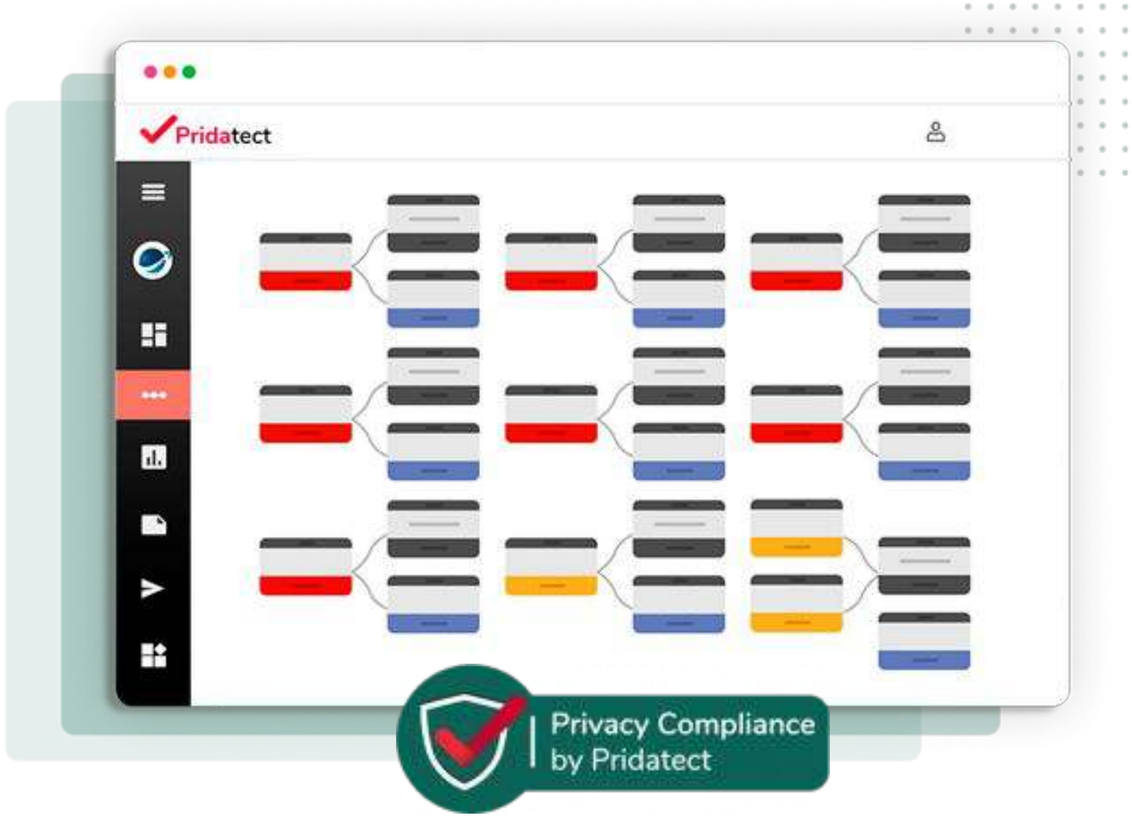
Detect and identify risks in your personal data processing (**customers, employees, suppliers...**). With the Pridatect platform we can identify and analyse the threats and vulnerabilities in your processes.

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 a constant 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 the 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 the data protection management in your educational organisation and ensure that your whole team has the necessary guidelines to protect the data of your students. 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

Lisa Hofmann

Chief of Legal Operations
Pridatect

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

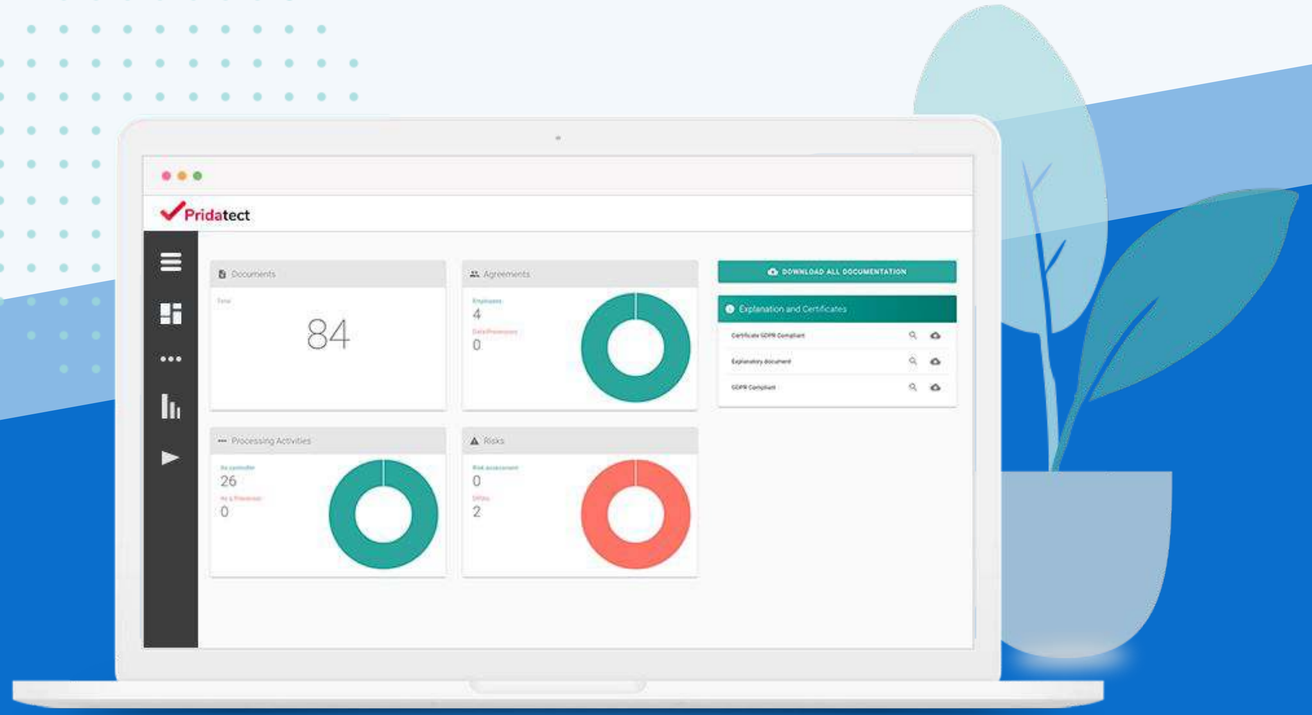
Ben Seretny

Data Protection Officer
DPO Centre

Certified Information Privacy Manager with a strong background in the pharmaceutical, healthcare and legal sectors.

Send us your questions!

lisa.hofmann@pridatect.com



Thanks for joining our webinar!

Key considerations during lockdown

Work with your vendors - choosing a product which suits your requirements and framework as well as the resources of your audience is key. What training is required, how accessible is the platform, how experienced are your IG team in the technology type.

Work with your audience - keep students and parents informed of any changes in software usage. This is always important to reduce potential complaints, but essential at a time when cyber security threats have risen.

Educate your users - implement policies or guidlines for safe use. Think about conduct as much as security.

Update your records of processing - consider a separate “Lockdown RoPA” if processing begins to deviate greatly from the norm.

Notify your data subjects on how their data will be used. Privacy notices need to be accurate and reflect any novel usage of personal data during the lockdown period.