Pridatect

# WEBINAR:
# GDPR After Brexit

# Your webinar hosts

## Lisa Hofmann

*Chief of Legal Operations & International DPO Pridatect*

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

## Rob Masson

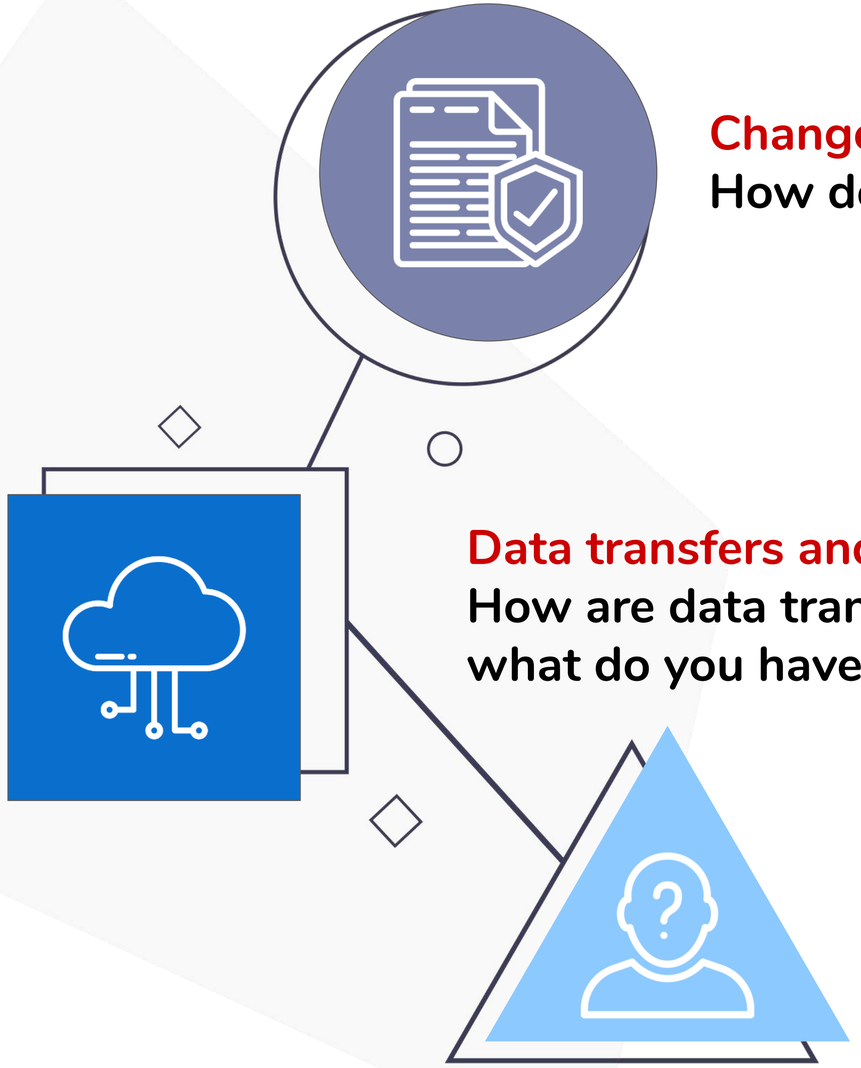
*Data Protection Specialist & CEO @The DPO Centre LTD*

Experienced UK data protection specialist, helping clients navigate GDPR compliance in the face of Brexit.

## *Nice to e-meet you!*

***Feel free to send your questions to lisa.hofmann@pridatect.com***

# Webinar Agenda: GDPR after Brexit



**Changes in data protection laws**
How does Brexit affect existing data protection laws?

**Data transfers and data storage**
How are data transfers between the UK and EU affected and what do you have to consider in terms of data storage?

**EU and UK representatives**
When do you need to appoint a representative and what is the representatives function?

# Brexit: What will happen to GDPR and data compliance?


How data is stored, transferred and processed between the UK & the rest of the EU will change.

The UK will have to demonstrate **adequacy**, meaning showing the EU that data is processed safely in the UK.

You **won't** need to appoint an EU representative **during the transition period** and data will continue to flow between the UK & the EU.

However, you **will** need an EU representative **after the transition period if you wish to do business with anyone in the EU.**

GDPR will be incorporated into existing UK data protection law as **UK GDPR**, so you should **take steps now to ensure you're compliant.**

***Fines for violating GDPR regulations can be as high as €20 Million or up to 4% of the companies annual revenue.***

# Which laws will change? Do I as a company have to comply with UK privacy laws and GDPR?

**There will be no immediate change** "*During the transition period there will be no immediate change to the UK's data protection standards. EU data protection laws, including the General Data Protection Regulation (GDPR), will continue to apply during the transition period alongside the Data Protection Act 2018..*" (Source: Gov.uk/guidance)

## But what does that mean? And what about afterwards?

- Essentially, the UK is being given time to achieve adequacy status in order to continue to able to work with stakeholders in the EU. In the event of not achieving adequacy status, EU law may still apply to certain types of data.

- Post the transition period, transfers from the EU to the UK will be subject to local transfer requirements in the senders country, and so you may have to comply with additional security measures.

- Possibly the most important point to takeaway is one we've already made: GDPR will likely be incorporated into existing data protection laws as the UK GDPR **and** you have to be compliant if you do business with **anyone** in the EU so **yes, you do have to comply with GDPR.**

***To define a policy for standard retention periods is not enough: Make sure to also put it into practice!***

# What happens when the UK becomes “a third country”?

The UK will have to demonstrate adequacy, meaning its data protection laws must be at least as robust as those set out by the EU in GDPR.  UK Investigatory Powers Act 2016 is a barrier to adequacy.

DPA 2018 will be amended to incorporate the UK GDPR.

# What is the current status of the adequacy decision?

In the case that the UK is not granted adequacy status, it is likely businesses would have to switch from any UK based cloud storage service providers.

**Standard Contractual Clauses** provide guarantees regarding data protection equivalent to that set out in GDPR.

Things seem to be leaning towards the granting of adequacy, permitting the free flow of personal data and is expected to be granted by the end of the transition period according to information from the European Commission (source: EC Publication Adequacy)

# What is the effect on international data transfers?

*There will be no change when transferring data from the UK to the EU.*

*HOWEVER*

*Data transferred from the EU to the UK will have to abide by the local requirements in the senders country. You must also be aware that data could conceivably become 'trapped' in the EU as processor to controller SCCs don't exist.*

***You will have to abide by GDPR if you wish to do business with members of the EU.***

***You may have to move your data from a UK cloud based storage provider***

***Ensure a safely designed migration to protect data during the process***

# Do I need to appoint an EU and or UK representative?

*When do I need to appoint one? What is the representative's role? What does the background of the representative need to be?*

- **You DON'T** need to appoint an EU representative during the transition period. **You WILL** need to appoint one once this transition period finishes (if you're outside the EEA that is).

- **The role of the representative** is to **be the point of contact for data subjects and regulators & maintain records of processing activities (RoPA).**

- A representative should be established in one of the member states where processing takes place, so if subjects are only in (for example) Spain, then your Rep must be established in Spain.

# And what about penalties?

Penalties for GDPR breaches can and do happen, and fines can run into the **hundreds of millions**.

**Who can penalize me? The UK? The EU?**

- EU: European Data Protection Board (EDPB)

- UK: The ICO (The Information Commissioner's Office) can also give warnings, order bans and erasure of data.

According to (Art 83 GDPR) fines are administered by the individual member state supervisory authorities and takes into account 10 criteria:

- Nature of infringement
- Intention
- Mitigation
- History
- Cooperation
- Data Type
- Notification
- Certification
- Other (ex. financial impact on the firm from the infringement)

***Violations take into account 10 criteria, and can be punished by supervisory bodies in the UK & the EU.***

# Actionable steps that must be taken

- Review your EU lead authority
- Review data transfers in/out of UK and onwards
- Review the legal basis for transfers
- Review the need for EU and or UK representatives
- Review risk and get DPIAs into place
  (regulators have stated not an enforcement priority in the short term)
- Amend privacy notices & records of processing
- Amend breach notification protocols

***The seven steps presented here are tasks you can and should perform immediately in order to ensure you're GDPR compliant post Brexit.***

# How do you ensure GDPR compliance?

To protect your data and comply with GDPR data storage is of course not the only concern. To implement an adequate data protection concept, you need to:

- Perform a **data protection compliance analysis** to detect potential dangers of GDPR violations
- Create a **directory of processing activities** to correctly answer to data subject requests
- Conduct a **GDPR risk analysis** that helps define measures to close data protection gaps
- Define **technical and organisational measures** that minimize future risks

Prepare in good time to avoid GDPR breaches!

# What does the implementation of a data protection concept often look like in reality?

**Creation of document folders** to collect contracts, documents, processes, etc. These have to be updated manually on a regular basis. Certain data must be deleted regularly.

**Excel lists** with processing activities, TOMs (technical and organisational measures) etc., which are sent back and forth between employees in different versions

**Email communication** to collect information from various business areas and employees

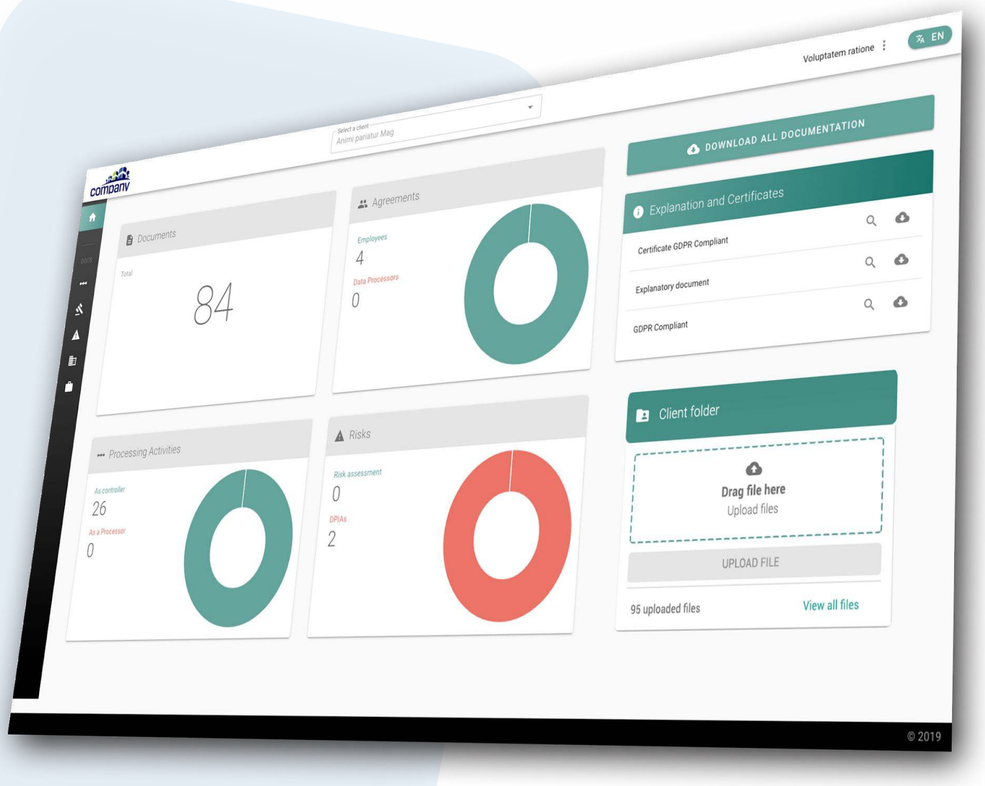
***Consider the risks:***

- ***Error prone***
- ***Unsecured***
- ***Lack of overview***
- ***Time and effort intensive***

# The alternative: A software for privacy compliance

## Privacy compliance simplified:

Manage your data protection easily in a collaborative cloud environment




### Become GDPR compliant

All required documentation and information available when needed to demonstrate that your company complies with current regulations.

### Control over all data processes

Keep total control of all the data your company is managing in a visual and intuitive way.

### Legal assisted intelligence solution

Our intuitive data compliance workflows assist your data protection from document automation to privacy impact assessments.

# Everything you need for a successful privacy program

## Trusted technology solution for your data protection

With all the functionalities you need

### Risk Assessment

Mitigate data protection risks

### Impact Evaluation (PIA)

Automated privacy impact assessments

### GAP Analysis

Identify gaps in your data protection

### Processing Activities

Keep an updated registry of processing activities

### Data Mapping

Map all of your companies data flows

### TOMs

Define risk reducing technical and organisational measures

### Privacy reports

Generate automated privacy reports

### International transfers

Manage data transfers internationally

### Data breach management

Successful reactive management for data breaches

### Website compliance

Generate privacy policies, cookie policies, terms & conditions

### Subjects access rights

Manage consumer and subject rights requests

### Secure Cloud Userdesk

Collaborate on our secured cloud environment

### External DPO service

Get a virtual DPO for your company

### Vendor contracts

Generate GDPR compliant vendor contracts

### Legal document automation

Create legal documents based on our models

# Test Pridatect for yourself!

Take control of the data protection management in your company and protect yourself from GDPR penalties. We help you to detect risks and put the right technical and organizational measures into place to protect your data.

Contact us now for a Free Demo or make use of the Pridatect Free Trial for 7 days.

Schedule your free demo

# Thank you for joining our Webinar!