HARTLEY

BEAUTY & TRAINING

GDPR

What is General Data Protections Regulation (GDPR)?

- The General **Data Protection Regulation** (**GDPR**) is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union.

- The General Data Protections Regulation (GDPR) is a ruling intended to protect the data of citizens within the European Union. The GDPR is a move by The Council of the European Union, European Parliament, and European Commission to provide citizens with a greater level of control over their personal data.

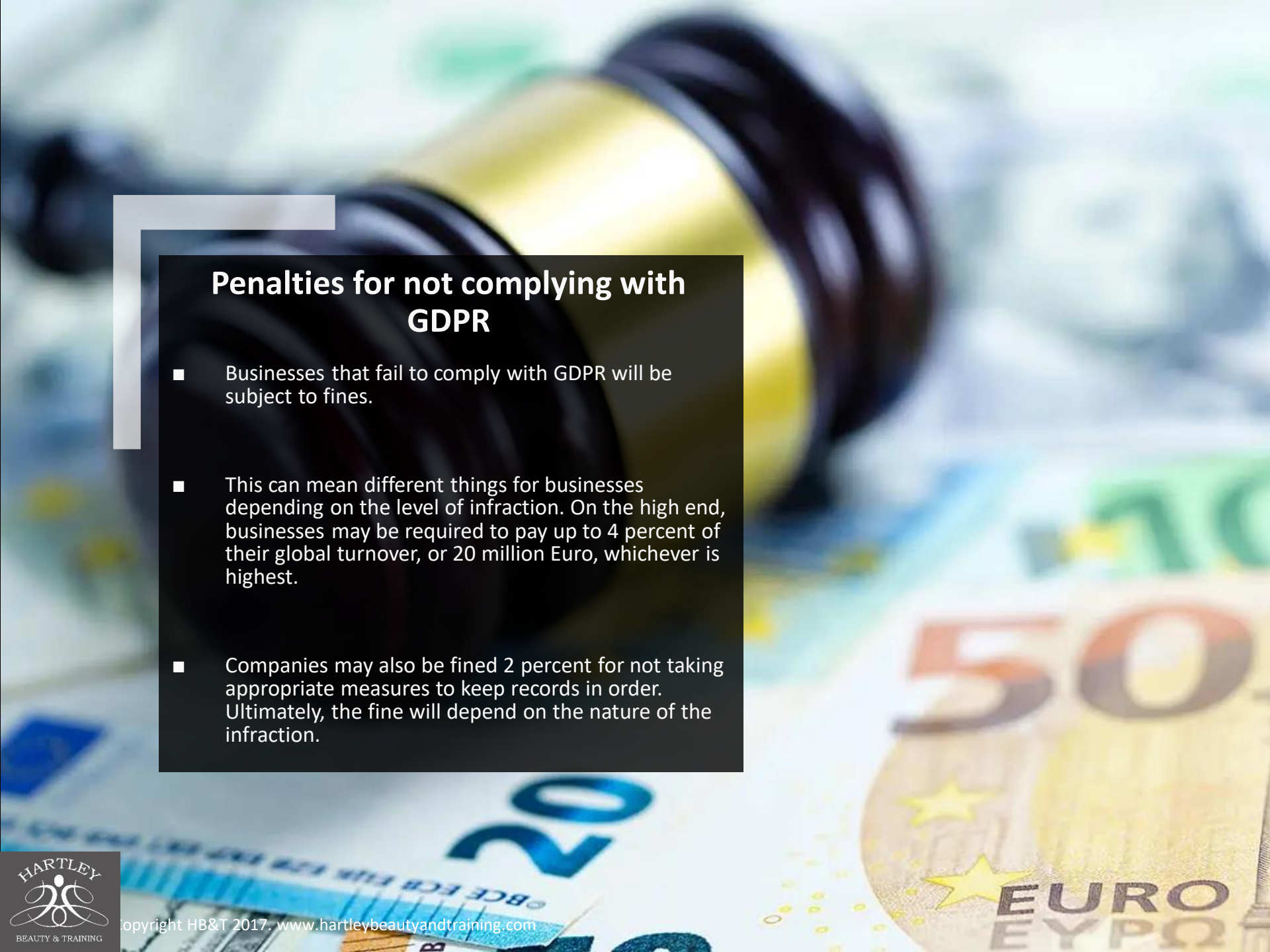
Who will be affected by the GDPR?

- The GDPR has far-reaching implications for all citizens of the European Union and businesses operating within the EU, regardless of physical location.
- If businesses hope to offer goods or services to citizens of the EU, they will be subject to the penalties imposed by the GDPR.
- In addition, any business that holds personal data of EU citizens can be held accountable under the GDPR.

HARTLEY
BEAUTY & TRAINING

What sort of data will fall under the General Data Protections Regulation?

- Name
- Photo
- Email address
- Social media posts
- Personal medical information
- IP addresses
- Bank details



Penalties for not complying with GDPR

- Businesses that fail to comply with GDPR will be subject to fines.
- This can mean different things for businesses depending on the level of infraction. On the high end, businesses may be required to pay up to 4 percent of their global turnover, or 20 million Euro, whichever is highest.
- Companies may also be fined 2 percent for not taking appropriate measures to keep records in order. Ultimately, the fine will depend on the nature of the infraction.

GDPR: DATA PROTECTION AND RISK DETECTION CHECKLIST

The GDPR impacts any organisation that does business with or holds data on individuals in the 28 countries in the EU. With compliance mandatory for May 2018, here is a 10 step guide to help you:

1. **Research** to understand your firm's exact responsibilities as related to the regulation.

2. **Complete a risk assessment** on the systems used for processing and controlling data by your firm, any vendors or other 3rd party providers.

3. **Understand whether you need to appoint a Data Protection Officer** to take responsibility and control of data protection issues on behalf of your firm.

4. **Identify the biggest areas of risk** and prioritise systems that hold sensitive personal information.

5. **Speak to experts** and make use of advisory services, to ensure you are fully meeting all GDPR requirements.

6. **Create an action plan**, which lays out all the tasks that need to be completed prior to implementation of the GDPR in 2018.

7. **Investigate innovative and specialist technology** and select a solution specifically designed to support business services firms, which can facilitate normal workflow, while preventing data loss and providing risk detection analytics.

8. **Use a data removal solution** to strip files of sensitive metadata before they are uploaded to, or shared in a browser, the cloud or via email.

9. **Identify a solution** that can help assess the risk from content being shared and make sure files are only shared in correct and sanctioned locations, with flags on unsanctioned activity.

10. **Educate staff and end users** on the risks of data sharing and particularly of embedded data within files being shared.

Glossary of Terms

TERM	MEANING
Personal Data	Data relating to an individual, such as: phone numbers, email addresses, names, other contact details, information about health and/or lifestyle, etc.
Lawful Basis	A legal reason for doing something, in this case processing personal data
Privacy Notice	The part of the terms and conditions you hand out to anyone you collect data from that explains why you are collecting their data, what you will do with it, etc.
Legislation	A set of laws, considered collectively
Data Processing	A broad term that encompasses: collecting data, storing data, analysing data, or using data for any purpose.
Compliance	Acting in accordance with something, in this case the law.
Automated decision-making tools	Technology that makes decisions by analysing data without human input.

What personal information may we hold about our clients?

- Full name
- Telephone number
- Email address
- Treatment details
- Medical history
- Payment history

Where and how should clients details be stored?

- Locked cabinet (stored for 7 years)

- On a computer which is password protected