Faria Education Group

Is your Data safe?

A Simple guide to Data Protection within a Remote Learning Environment

Faria Education Technology Conference

March 1-5, 2021

"The oldest computer can be traced back to Adam and Eve, Surprise, Surprise, it was and Apple, but with extremely limited memory, just ONE byte and everything crashed!"

Peregrine R Perrott

Global Data Protection Officer
Faria Education Group

#FEGTechConf

Data Protection is not that boring REALLY !!

"Kathy, if you agree to these terms of service, click 'I do.'"

"Before I write my name on the board, I'll need to know how you're planning to use that data."

Faria Education Group

What Does the GDPR Mean for

GLOBAL DATA PROTECTION?

What is the GDPR?

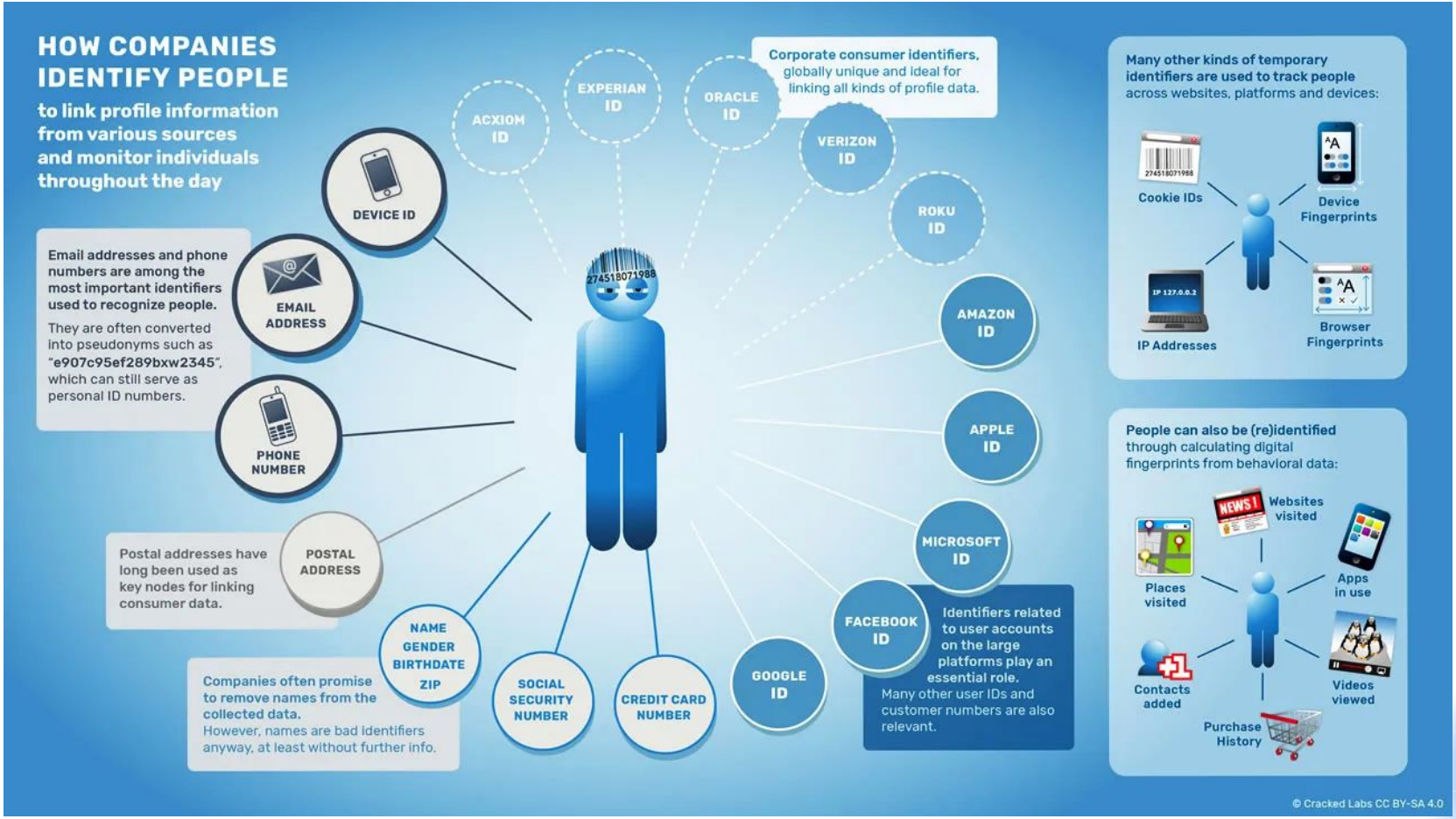
The General Data Protection Regulation (GDPR) is designed to:

HARMONIZE DATA PRIVACY laws across Europe

PROTECT AND EMPOWER all EU citizens' data privacy

RESHAPE the way organizations across the region approach data privacy[1]

#FEGTechConf


HOW COMPANIES IDENTIFY PEOPLE
to link profile information from various sources and monitor individuals throughout the day
ACXIOM ID
EXPERIAN ID
ORACLE ID
Corporate consumer identifiers, globally unique and ideal for linking all kinds of profile data.
VERIZON ID
ROKU ID
DEVICE ID
Email addresses and phone numbers are among the most important identifiers used to recognize people.
They are often converted into pseudonyms such as "e907c95ef289bxw2345", which can still serve as personal ID numbers.
EMAIL ADDRESS
PHONE NUMBER
274518071988
AMAZON ID
APPLE ID
MICROSOFT ID
FACEBOOK ID
Identifiers related to user accounts on the large platforms play an essential role.
Many other user IDs and customer numbers are also relevant.
Postal addresses have long been used as key nodes for linking consumer data.
POSTAL ADDRESS
NAME GENDER BIRTHDATE ZIP
Companies often promise to remove names from the collected data.
However, names are bad identifiers anyway, at least without further info.
SOCIAL SECURITY NUMBER
CREDIT CARD NUMBER
GOOGLE ID
Many other kinds of temporary identifiers are used to track people across websites, platforms and devices:
Cookie IDs
Device Fingerprints
IP Addresses
Browser Fingerprints
People can also be (re)identified through calculating digital fingerprints from behavioral data:
Websites visited
Apps in use
Places visited
Videos viewed
Contacts added
Purchase History
© Cracked Labs CC BY-SA 4.0

Data Protection Act 2018 and Schools

The Data Protection Act (DPA) was designed to protect the privacy of individuals. When the DPA was updated to the GDPR in May 2018, the regulations around data protection changed throughout Europe. Schools handle what the GDPR classifies as ‘special category data,’ detailing pupil information such as ethnicity, race, biometric data, and trade-union membership in some instances. This data is subject to strict controls, and therefore, schools need to adhere to GDPR guidelines and protect this information efficiently.

The processing of personal data stored on school websites, paper, servers, and databases is all covered by GDPR. Critically, schools must undertake stringent data protection impact assessments when they upgrade their software, change IT infrastructure, or introduce new technology that deals with personal data. Note that GDPR compliance is a legal obligation, making it illegal if your school fails to produce precise documentation that proves effective management of all information systems. Penalties are delivered on a case-by-case basis, with the maximum fine for non-compliance set at €20million (roughly £17.5 million).

What is Personal Information?

Personal information can be defined as anything relating to an individual that identifies them. This applies to both physical and digital records.

Examples of personal information that a school may store include:

- Names and dates of birth for both staff and pupils.
- Images of staff and pupils that confirm their identity and can be linked to additional personal information.
- National Insurance numbers.
- Addresses of staff and pupils.
- Recruitment information.
- Financial records, such as tax information and bank details.
- Information relating to pupil behaviour and school attendance.
- Medical records, including GP names and medical conditions.
- Exam results and class grades.
- Staff development reviews.
- School assessments and marks.
- Safeguarding information, including data related to SEN assessments.

With such a myriad of personal information held by schools, the importance of protecting such data is paramount.

Q: Is there anything else you would class as personal information?

What are the Key Principles in Law

Lawfulness, fairness, and transparency

Data minimisation

Purpose limitation

Accuracy

Storage limitations

Integrity and confidentiality

Accountability

Faria Education Group

Potential security measures for school data protection include

- The use of strong passwords.
- Encryption of all personal information stored electronically.
- Shredding of all physical copies of confidential waste.
- Installation of virus checking software and firewalls on school computers.
- Turning off all ‘auto-complete’settings.
- Limiting access to personal information wherever necessary.
- Holding telephone calls in designated private areas.
- Ensuring that all storage systems are secure.
- Keeping digital devices locked away securely when not in use.
- Making sure that all papers and devices containing sensitive information are stored securely

Q: What do you do in your areas? (5 min discussion)

Faria Education Group

Ask yourself these questions HONESTLY!

- *Does your school have a Use Policy in place?*
- *Has a Data Protection Policy been implemented throughout the school?*
- *Do you monitor the use if school internet, intranet, and any accessible chat rooms and regulate their use?*
- *Do you have restrictions in place to prevent access to inappropriate websites and materials on the school internet and network?*
- *Do you teach internet safety as part of your school curriculum?*
- *Do you have a reporting procedure in place in case inappropriate materials or websites are accessed?*
- *Do you follow strict safety guidelines when publishing names or images of students on your school website?*
- *Do you send information to parents via email?*

Evidence of inadequate data protection practices or guidelines includes lack of internet monitoring or filtering, little or no e-safety education in place, and students with no awareness of how to report data-sensitive problems.

How to undertake a School Audit

To guarantee that all information is vetted for accuracy, stored only for the time that it is relevant, and stored securely, annual audits should be carried out.

To conduct an audit, you should:

- Monitor all 'live' files to make sure they are updated and accurate.
- Send out a letter at the beginning of each school year urging parents and pupils to check that all of their personal details are correct. This is a great way to avoid emergencies; especially when emergency contact information is out of date.
- Amend all information that is inaccurate immediately.
- Destroy all personal data that is no longer needed or out-of-date. This could involve deleting computer files, shredding documents, or formatting hard drives securely so that all information is permanently erased and inaccessible.
- Adhere to the disposal of records schedule, which states the duration that certain types of personal information can be retained before they must be destroyed. Note that some stipulations are legally required while others are recommended for best practice.
- If your school holds any personal data for longer than it is required, you violate the Data Protection Act.

Q: Do you think this is something that can be achieved ?
Q: Do you have Senior Team support for this?

Summary

2020 brought several major developments in the world of data protection legislation. Most notably, the California Consumer Privacy Act (CCPA) came into force in January in the United States and the Court of Justice of the European Union (CJEU) ruled in the Schrems II case that the European Commission's adequacy decision in regards to the EU-US Privacy Shield was invalid, effectively putting an end to free data flows between the United States and the EU.

2021 is set to be an exciting one for privacy protection legislation as several notable privacy laws will begin enforcement, with several others falling in line to the new international standard set by the GDPR. Cross-border transfers are likely to be one of the big compliance issues being tackled by legislative bodies and data protection authorities to ensure a regularization and normalization of data transfers between countries.

Faria Education Group

Thank you!

- Have questions? Email us at dpo@fariaedu.com
- The recordings will be available after the conference

Tweet Us @FariaEduGroup #FEGTechConf