Understanding the General Data Protection Regulation (GDPR) and its Implications for You

Eugene McKenna - European Campus Card Association
emckenna@ecca.eu
The General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy for all individuals within the European Union. It also addresses the export of personal data outside the EU.
What is GDPR

The General Data Protection Regulation (GDPR) is in force as of the 25th May 2018, replacing the existing data protection framework under the EU Data Protection Directive.
Is there a Major Change?

The right to be informed is an integral element of transparency under the GDPR. It is about being clear and open with individuals about how you collect and use their personal data.
The Seven Key Principles of GDPR

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability
What is Personal Data

Data relating to a living individual who is or can be identified either from the data or in conjunction with other information that is in.
What Constitutes Data Processing

Processing covers a wide range of operations performed on personal data, including by manual or automated means. It includes the collection, recording, organization, structuring, storage, dissemination...........
Examples of Processing Data

- Staff HR and payroll admin
- Campus card personalization data
- Access control data
- Transactional management data
- Sending promotional emails
- Posting/putting a photo of a person on a website
- Storing IP addresses or MAC addresses
- Video recording (CCTV)
Data Controllers & Processors
Duties

Data Controllers

Data Processors
Role of Data Controllers

The controller is the person or business who determines the purpose for which, and the way in which, personal data is processed.
Role of Data Processors

The processor is a person, public authority or other body which processes personal data on behalf of the data controller.
Will GDPR affect Universities and Businesses outside the EU

Every organization & university, that processes or monitors EU residents’ data must comply with GDPR. Even if they are not established in the EU, they will still have to comply with GDPR when processing an EU residents’ personal data.
An Understanding of GDPR

Consent
What’s new?

When is consent appropriate?

What is valid consent?

How do we get consent?
Granular and separate
Granular and separate

What does 'granular’ mean?

- Separate consent for separate things
- Separate from your terms and conditions
- Specific to your purposes and methods
Unambiguous and clear affirmative action
Unambiguous affirmative action

It must be obvious that they intended to consent – there can be no doubt.

A clear affirmative action means a clear action to opt in.
No pre-ticked opt-in boxes
No pre-ticked opt-in boxes

Don’t use pre-ticked opt-in boxes...

...or rely on any other form of silence, inactivity, or consent as the default
Identity of the controller
Identity of the controller

You must name your organisation

...and name any third party controller relying on the consent ..... Categories of third parties are not specific enough
Right to withdraw consent
Right to withdraw consent

Individuals have the right to withdraw consent at any time.

You must tell them this when you get consent.
Right to withdraw consent

Individuals have the right to withdraw consent at any time

It must be as easy to withdraw consent as to give it
Right to withdraw consent

Individuals have the right to withdraw consent at any time

You must stop processing as soon as possible
Clear records of consent
Clear records of consent

You will need to show:

Who consented...

When they consented...

What they were told...

How they consented
What’s new?

When is consent appropriate?

What is valid consent?

How do we get consent?
When **should** you use consent?

- There’s no other appropriate lawful basis
- You want to give people choice and control
- Or you are required to have consent
When **not** to use consent
When **not** to use consent

If you would do it anyway – asking for consent is misleading and inherently unfair

- If you are in a position of power – they may feel they have no choice
- If consent is a condition of service but not necessary for the service
Remember there are alternatives to consent.
• Contract with the individual
• Compliance with a legal obligation
• Protecting vital interests
• ‘Public task’ - official functions or public interest tasks laid down by law
• Legitimate interests
What’s new?

When is consent appropriate?

What is valid consent?

How do we get consent?
"Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"
Consent must be:

**Freely given**
(genuine choice & control)

**Specific and informed**
(targeted to your purpose & easy to understand)

**Unambiguous by a clear affirmative action**
(a clear signal that they agree)
Explicit consent
Explicit consent

Explicit consent is not very different from regular consent... however...

It must be affirmed in a clearly worded statement (either written or oral)...

Drink Me
Explicit consent

Explicit consent is not very different from regular consent... however...

It must specifically refer to the element of processing that requires explicit consent...
Explicit consent

Explicit consent is not very different from regular consent...

however...

A request for explicit consent should be separate from other consent requests.
Consent timescales
Consent timescales

There is no specific timescale for expiry of consent in the GDPR

How long consent lasts will depend on the context...

For example...
Consent timescales

There is no specific timescale for expiry of consent in the GDPR

The scope of the consent...
Consent timescales

There is no specific timescale for expiry of consent in the GDPR

The individual’s expectations...
There is no specific timescale for expiry of consent in the GDPR.

If the processing has evolved beyond the original consent.
Consent timescales

There is no specific timescale for expiry of consent in the GDPR.

And don’t forget consent can be withdrawn at any time – in which case you must stop the processing.
When is consent not consent?
For example, it’s not consent:

• If it’s not obvious that the individual has consented;

• If you can’t actually prove that you’ve got consent;

• If you weren’t named as seeking consent from the individual;

• If you used pre-ticked opt-in boxes or other methods where consent is the default;

or

If you’re not sure – as that means it’s not unambiguous!
What’s new?
When is consent appropriate?
What is valid consent?
How do we get consent?
Your consent request must be:

- **Prominent** – make it obvious
- **Separate and granular** – separate from T&Cs and separate consent for separate things
- **Concise** – don’t be vague or long winded and rambling
- **Easy to understand** – use plain language and don’t be confusing
As a minimum you must:

• Name your organisation

• Name any third parties who will be relying on the consent

• Explain your purposes and activities (what you’ll be doing and why)

• Tell people they can withdraw consent at any time
Methods of obtaining consent
Methods of obtaining consent

You can use a range of possible methods...

For example...

The individual signs a consent form...
Methods of obtaining consent

You can use a range of possible methods...

For example...

The individual ticks an opt-in box, either online or offline...
Methods of obtaining consent

You can use a range of possible methods...

For example...

The individual says ‘yes’ to a clear oral request for consent
Evidence of consent
Evidence of consent

You need evidence of:

Who

The individual’s name or other identifier (eg username, session ID)
Evidence of consent

You need evidence of:
Who
When

eg a dated document, electronic timestamp, or a note of the date and time of the conversation
Evidence of consent

You need evidence of:

Who
When
What

e.g., a master copy of the document with the consent request, or script that was used at the time
Evidence of consent

You need evidence of:

Who
When
What
How

eg a copy of the data capture form, the data submitted online (with timestamp), or a note of oral consent made at the time
Reviewing and refreshing
Reviewing and refreshing

Keep consent under regular review, and refresh if your purposes evolve beyond those originally specified.

There is no such thing as ‘evolving consent’ because consent must be specific.
Reviewing and refreshing

Keep consent under regular review, and refresh if your purposes evolve beyond those originally specified.

Consider whether to automatically refresh at appropriate intervals.
Reviewing and refreshing

Keep consent under regular review, and refresh if your purposes evolve beyond those originally specified.

How often you need to refresh consent will depend on the particular context and expectations.
Impact on Colleges & Universities
Impact on Colleges and Universities

7 Key requirements

1. Individuals have the right to access, correct and delete your data within 40 days of a request.
Impact on Colleges and Universities

7 Key requirements

Universities are required to rationalise data collection and review how long data is held.
Impact on Colleges and Universities

7 Key requirements

Data breaches will need to be disclosed to the supervisory body and individuals whose data is compromised within 72 hours of the breach.
Impact on Colleges and Universities

7 Key requirements

Universities will be required to prove permission has been obtained for use of data. Clarity and transparency of request for consent is essential.
Data protection prevention measures must be built into processes, policies and systems from the earliest stages of data collection.
Impact on Colleges and Universities

7 Key requirements

Universities will need to appoint a mandatory Data Protection Officer (DPO), forming part of the creation of an overall data protection strategy and programme.
Impact on Colleges and Universities

7 Key requirements

Universities will need to ensure that access to personal data is limited to only those who require it for legitimate purposes.
Penalties for breach of GDPR
Penalties for breach of GDPR

4% of Global Turnover or €20 million
More information is available...

https://eugdpr.org/
https://gdpr-info.eu/