
Preparing for GDPR:
What does it mean for Executive Search?
invenias

Data Privacy Today

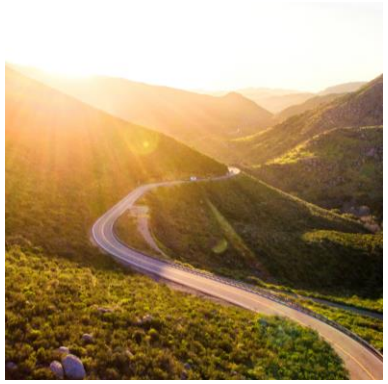
- EU Data Protection Directive 1995 and local legislation (e.g. UK Data Protection Act)
- Safe Harbour
- Model Clauses – technical and organisational measures
- Privacy Shield – US Jurisdiction

- GDPR – an essential update with significant expansion in scope and penalties.

GDPR Overview

- Penalties - greater of €20m or 4% of worldwide turnover
  - TalkTalk example (157,000; 16,000; £400k; £70m)
- Applies to Controller and Processor
- Accountability principle – requires you to show **how you comply** with the principles (next slide)
- Must have technical and organisation measures to ensure and demonstrate compliance
- Record keeping will be key
- Much stricter rules on reporting of data breaches to both the supervisory authority and, if required, to affected individuals
- Comes into application in EU from 25 May 2018 – the UK government is committed to that date
- Data protection by Design and Data Privacy Impact Assessments

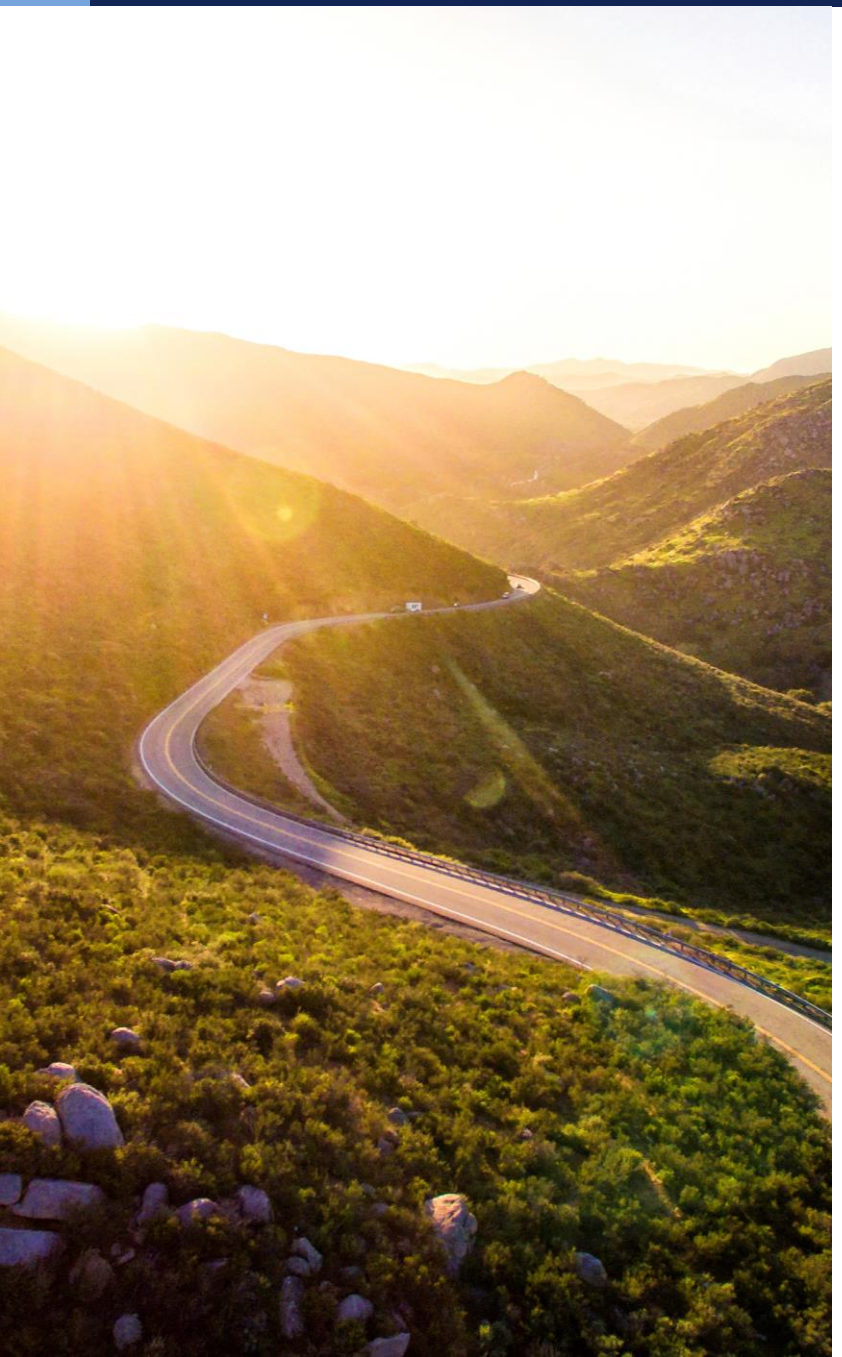
GDPR in 3 words – The Three Cs



Compliance

Consent

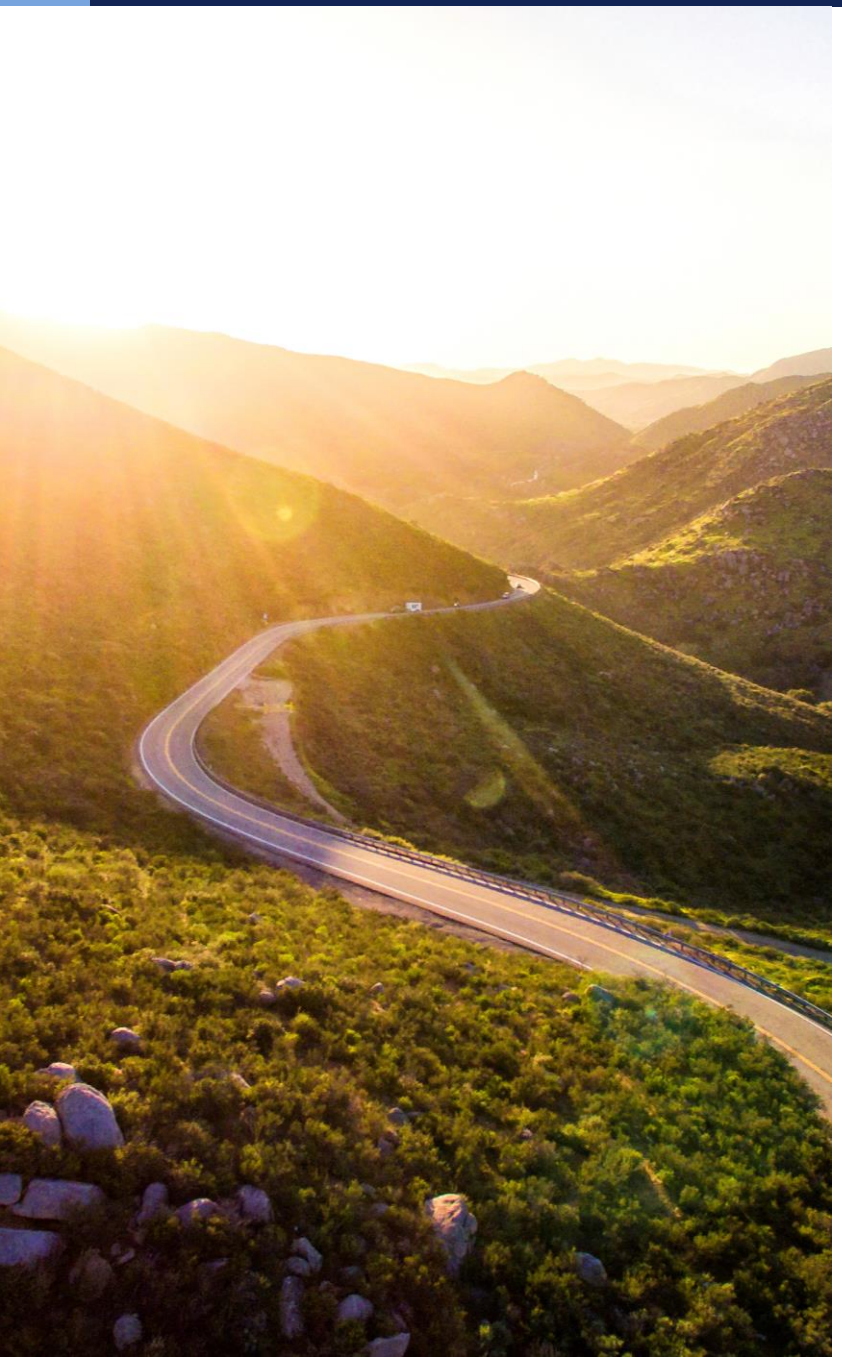
Communication



The Principles of Personal Data under GDPR

- Lawfully, fair and transparent
- Purpose
- Necessary
- Accurate
- Secure

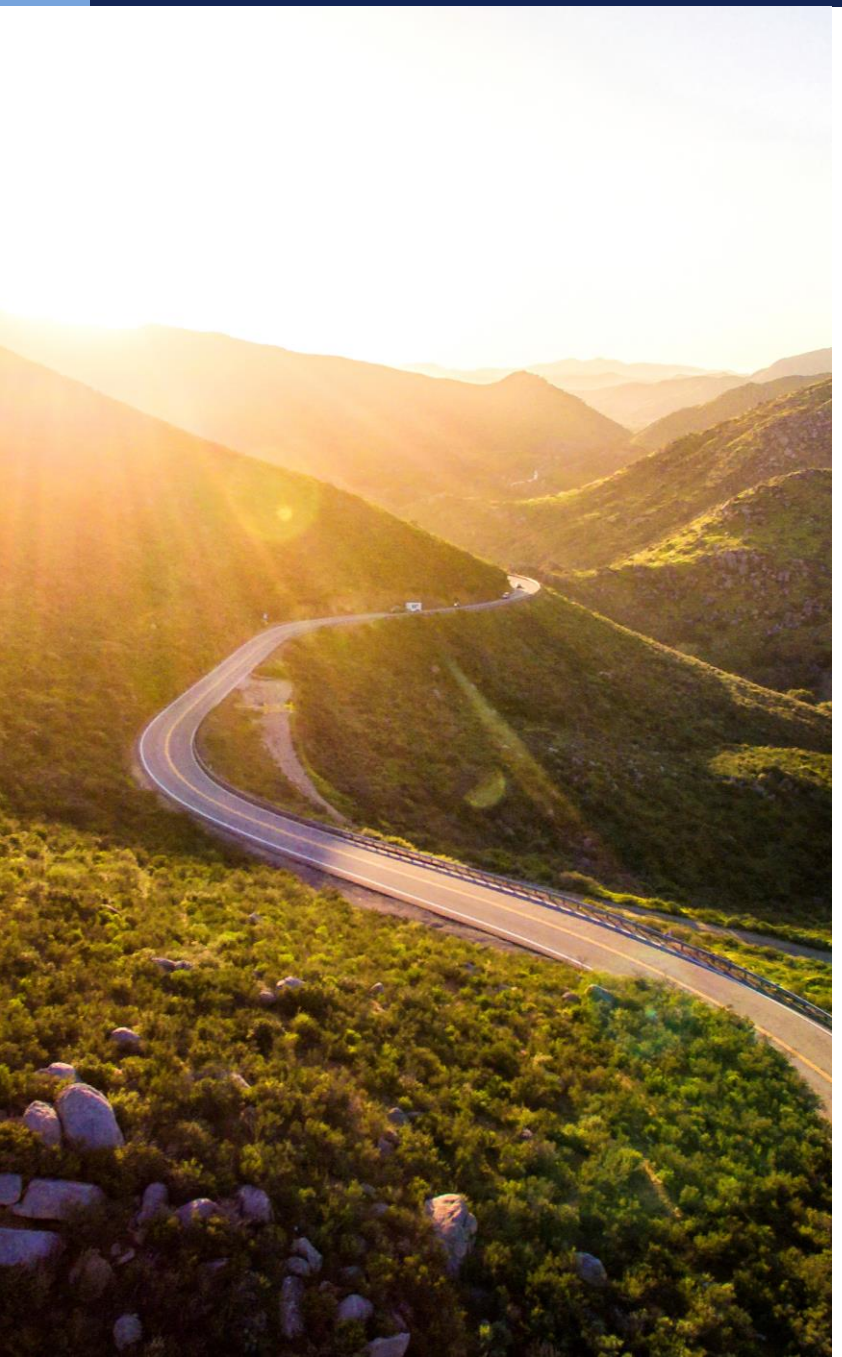
personal data shall be processed **lawfully**, **fairly** and in a **transparent** manner in relation to individuals. Lawful processes include "consent", "contractual necessity" and "legitimate Interest"



The Principles of Personal Data under GDPR

- Lawfully, fair and transparent
- Purpose
- Necessary
- Accurate
- Secure

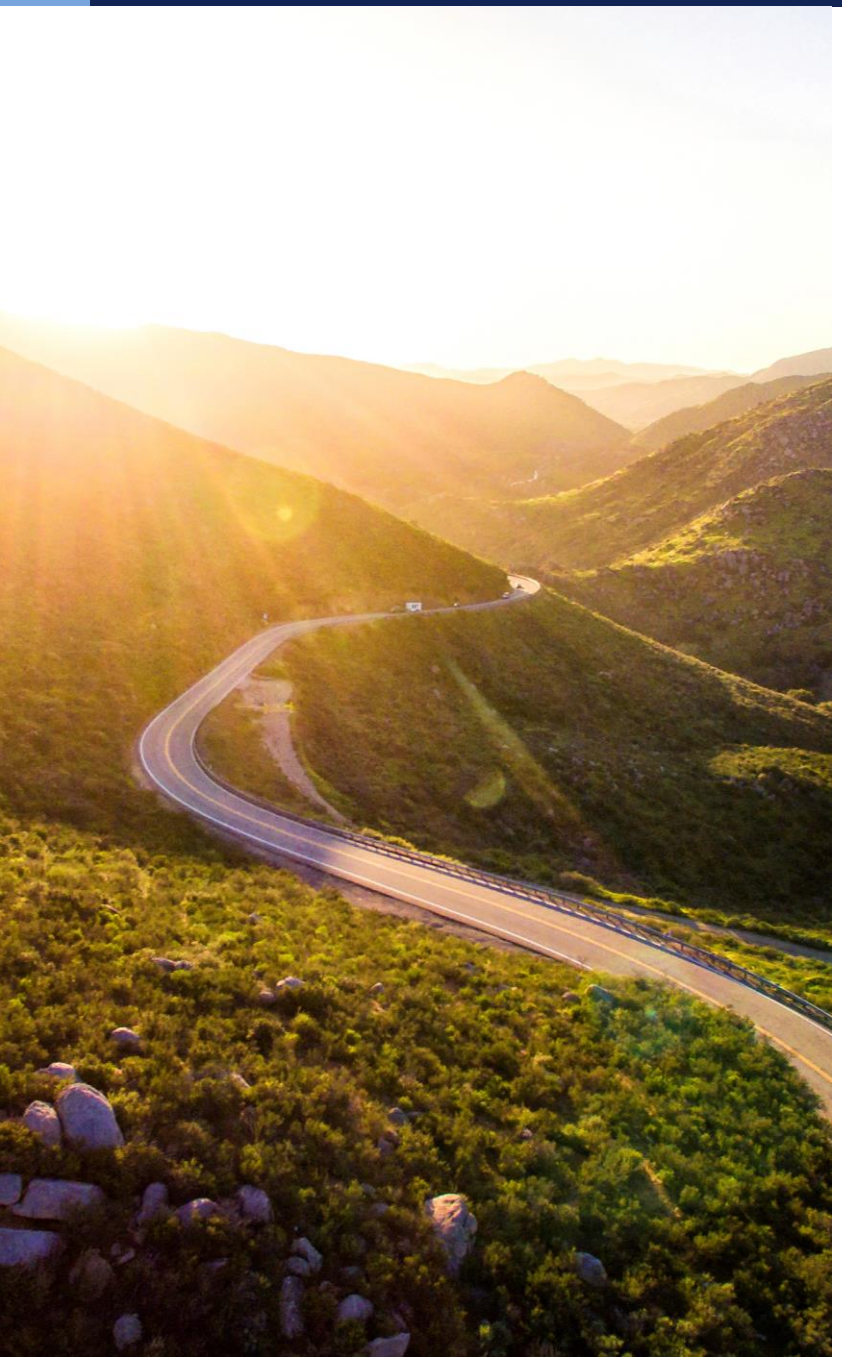
personal data shall be collected for **specified**, explicit and **legitimate purposes** and not further processed in a manner that is incompatible with those purposes



The Principles of Personal Data under GDPR

- Lawfully, fair and transparent
- Purpose
- Necessary
- Accurate
- Secure

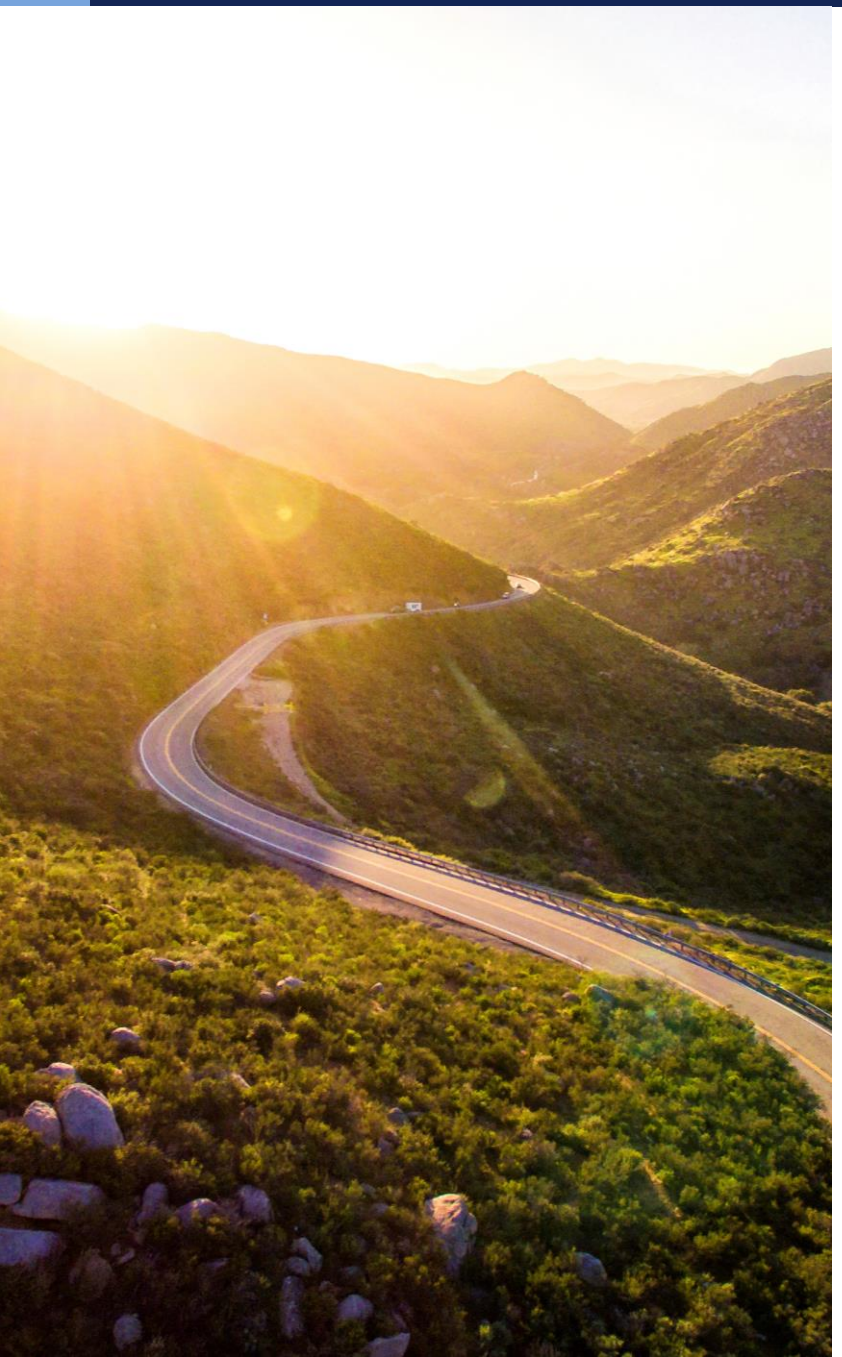
personal data shall be **adequate**, **relevant** and **limited** to what is **necessary** in relation to the purposes for which they are processed; and kept in a form which permits identification of data subjects for **no longer than is necessary** for the purposes for which the personal data are processed



The Principles of Personal Data under GDPR

- Lawfully, fair and transparent
- Purpose
- Necessary
- Accurate
- Secure

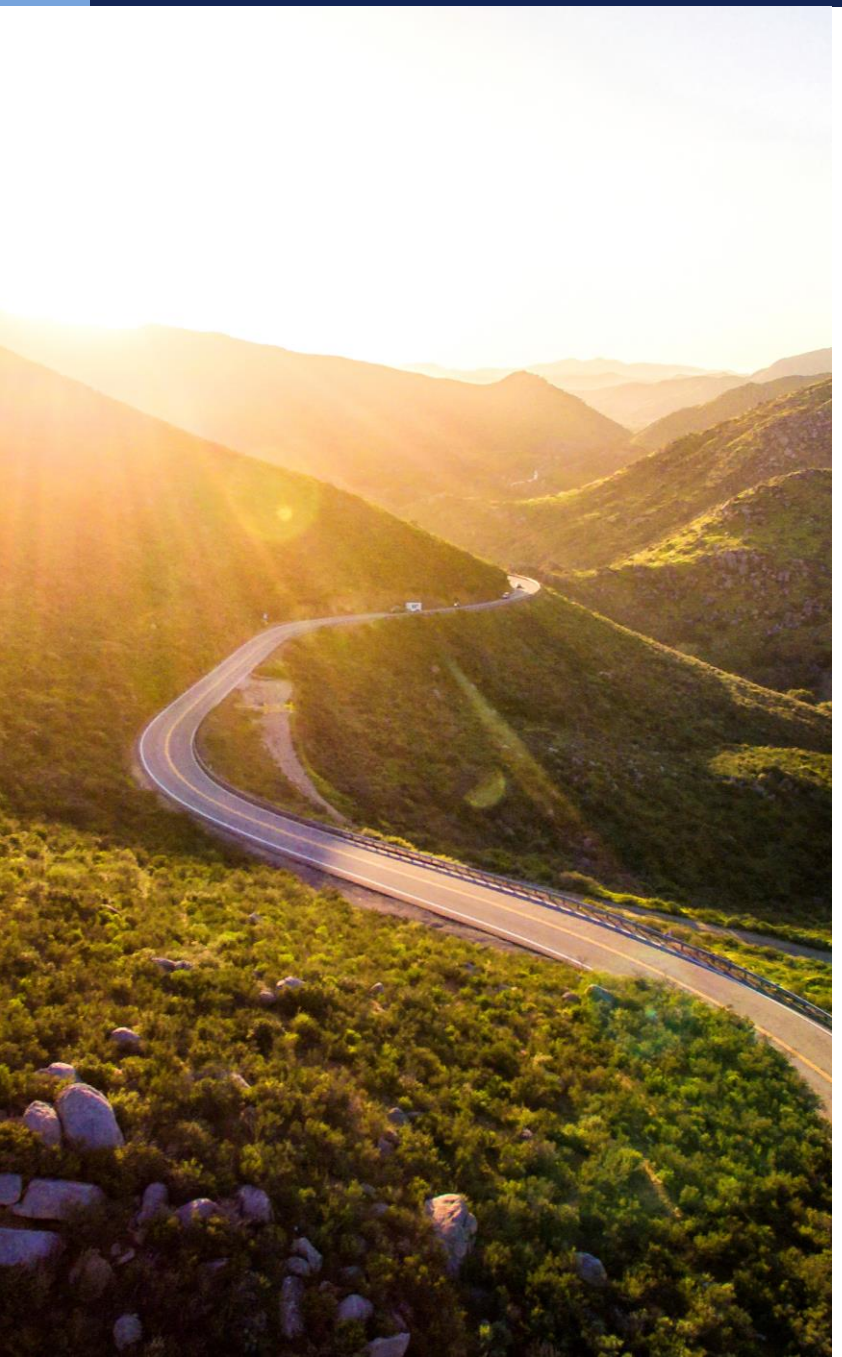
personal data shall be **accurate** and, where necessary, kept **up to date**



The Principles of Personal Data under GDPR

- Lawfully, fair and transparent
- Purpose
- Necessary
- Accurate
- Secure

personal data shall be processed in a manner that ensures **appropriate security** of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures



The Principles

- Article 5 of the GDPR requires that personal data shall be:

a) processed **lawfully**, **fairly** and in a **transparent** manner in relation to individuals;

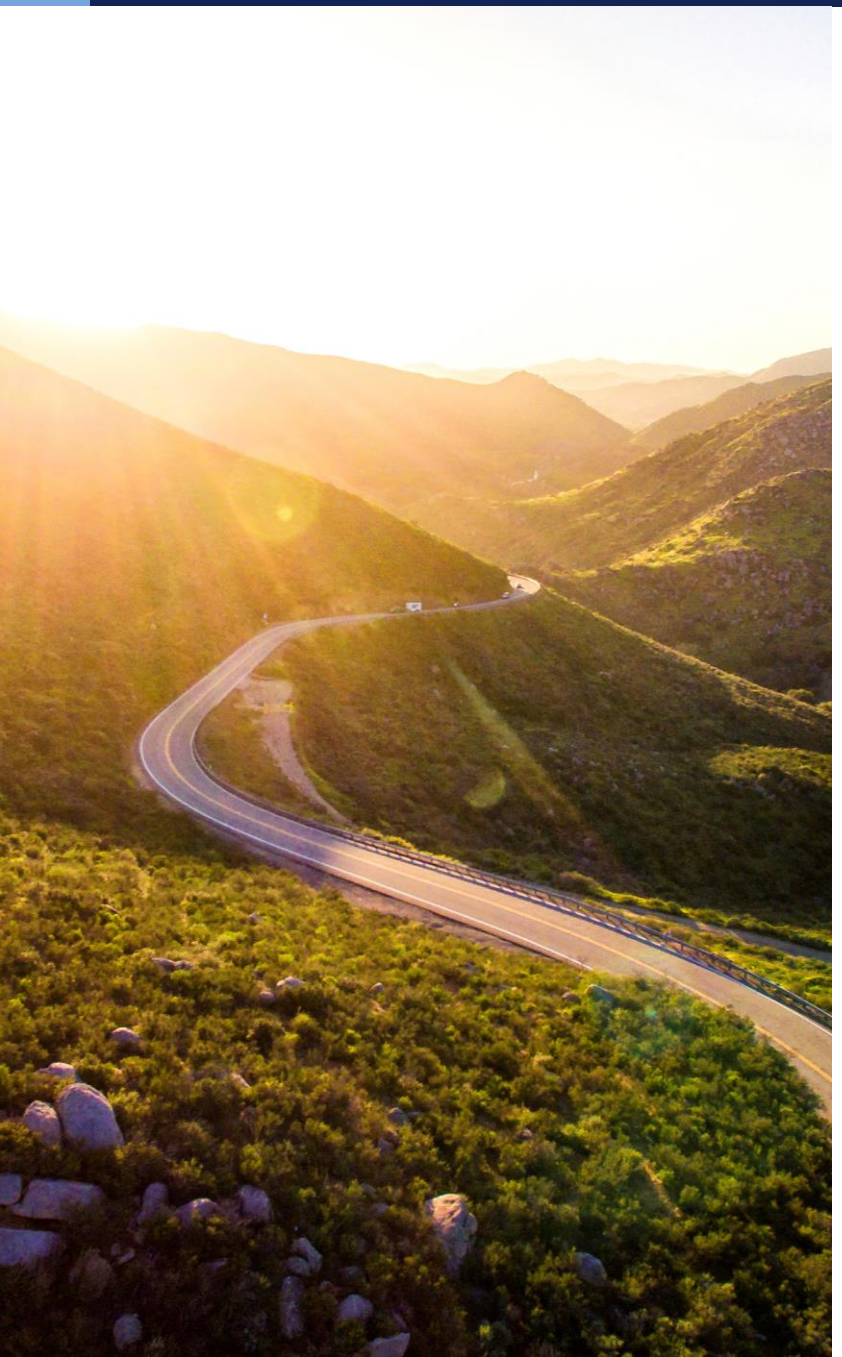
b) collected for **specified**, explicit and **legitimate purposes** and not further processed in a manner that is incompatible with those purposes;

c) **adequate**, **relevant** and **limited** to what is **necessary** in relation to the purposes for which they are processed;

d) **accurate** and, where necessary, kept **up to date**;

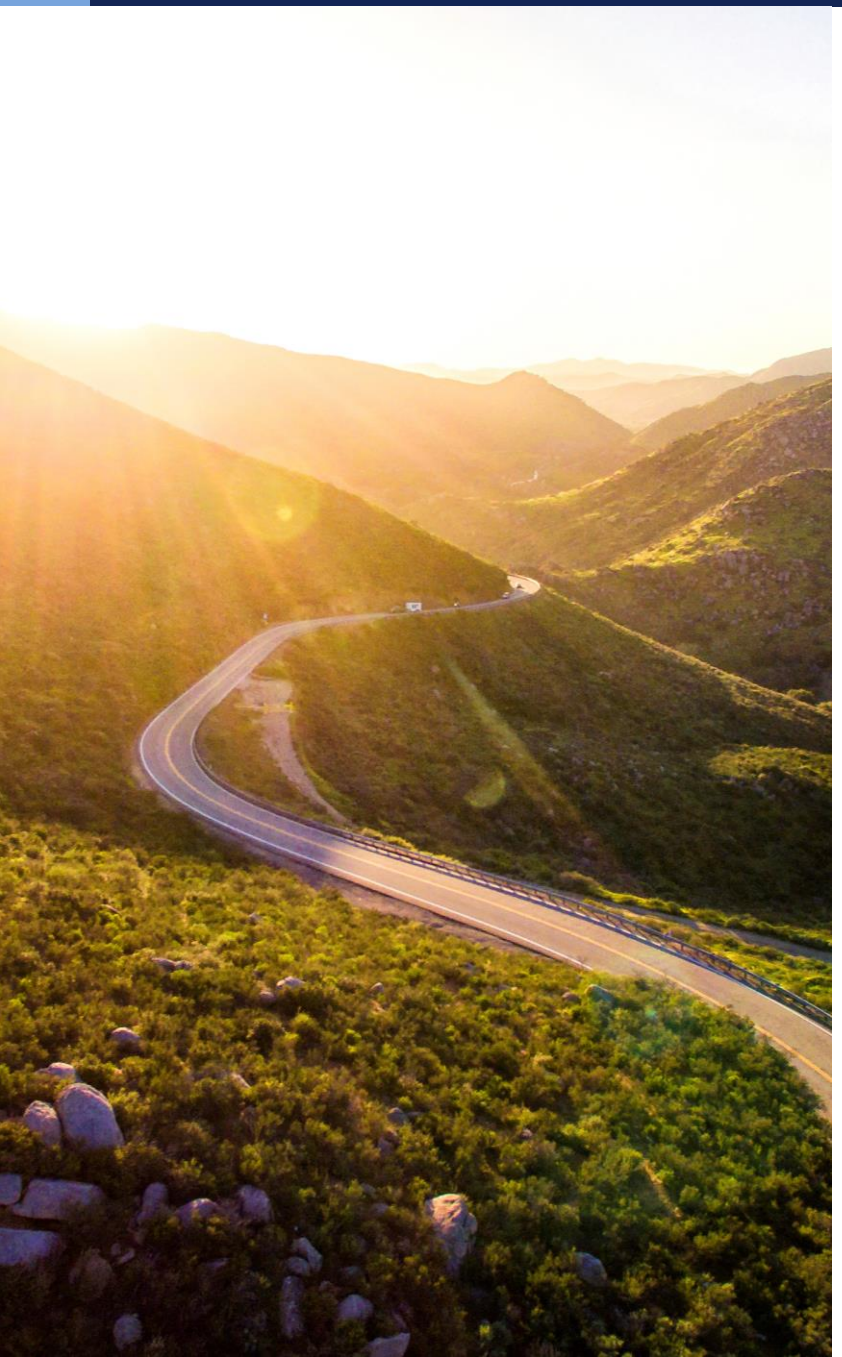
e) kept in a form which permits identification of data subjects for **no longer than is necessary** for the purposes for which the personal data are processed;

f) processed in a manner that ensures **appropriate security** of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.



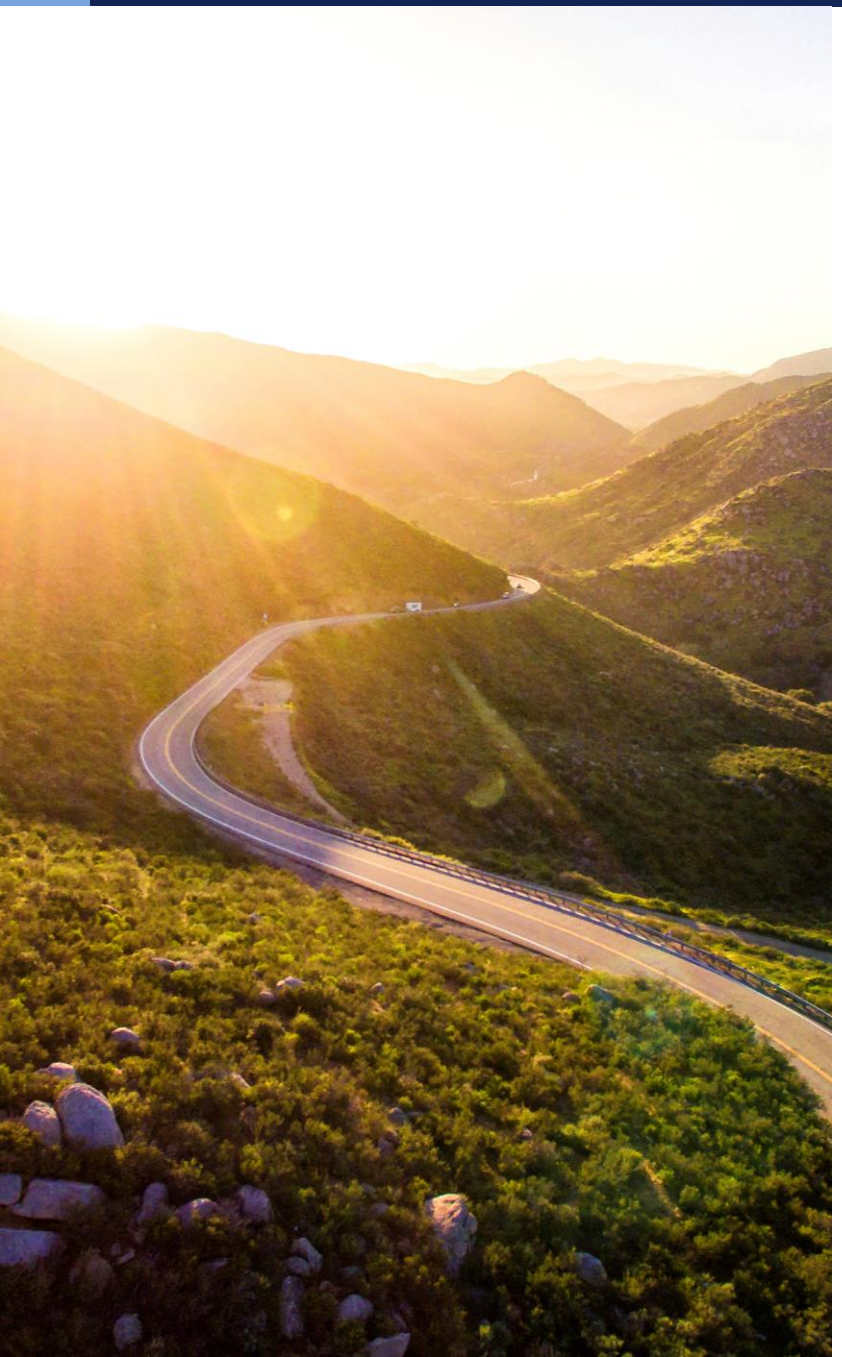
Compliance

- Article 5(2) requires that:
- "the controller shall be responsible for, and be able to demonstrate, compliance with the principles."



Accountability and Governance

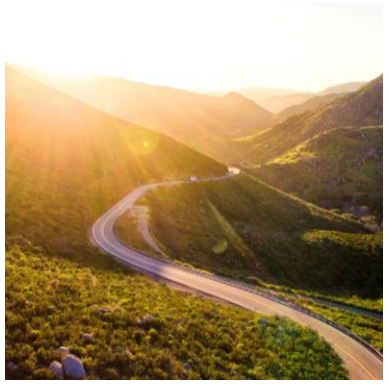
- The GDPR includes provisions that promote accountability and governance
- While the principles of accountability and transparency have previously been implicit requirements of data protection law, the GDPR's emphasis elevates their significance
- This highlights that you must be able to demonstrate you comply and understand your responsibilities (and those of your staff)



Data Protection by Design and Default

- Data protection by design must be at the **heart** of everything you do
- You now have an **obligation** to implement technical and organisational measures to show that you have considered and integrated data protection into your processing activities
- Fines – up to €20m or 4% of your global turnover for non compliance

GDPR in 3 words – The Three Cs



Compliance

Consent

Communication

GDPR Personal Data

- "**Personal Data**" is currently defined as "any information relating to an identified or identifiable natural person" and this includes both 'direct' and 'indirect' identification
- The Directive adds "an identification number or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"
- The GDPR introduces specific definitions of "genetic data" (e.g. an individual's gene sequence) and "biometric data" (i.e. fingerprints, facial recognition, retinal scans etc.)

Consent

- Consent must be:
  - freely given, specific, informed and unambiguous
  - a statement or clear affirmative action (recorded)
  - easy for candidates through a portal
  - more difficult to research
- Matters prohibited without explicit consent:
  - racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data for the purpose of uniquely identifying a natural person; data concerning health; data concerning a natural person's sex life or sexual orientation
- "Silence, pre-ticked boxes or inactivity" is presumed inadequate to confer consent – opt-in rather than opt-out

Legitimate Interest

- Whilst "consent" is one of the lawful bases on which personal data can processed it is also one that can be difficult to achieve and it also confers additional rights on the individuals.
- The ICO (UK Information Commissioners Office) in a discussion paper in March 2017 have proposed that for many situations it will be better to use the lawful basis of "legitimate interest" to justify the storing and processing of personal data.
- "Silence, pre-ticked boxes or inactivity" is presumed inadequate to confer consent – opt-in rather than opt-out

Withdrawal of Consent

- An individual can withdraw their consent at any time
- Right to Erasure

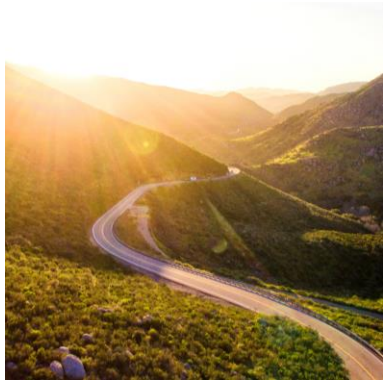
Currently

- right to erasure is limited to processing that causes unwarranted and substantial damage or distress

Under the GDPR

- this threshold is not present – it can be for any reason
- however, if the processing does cause damage or distress, this is likely to make the case for erasure stronger

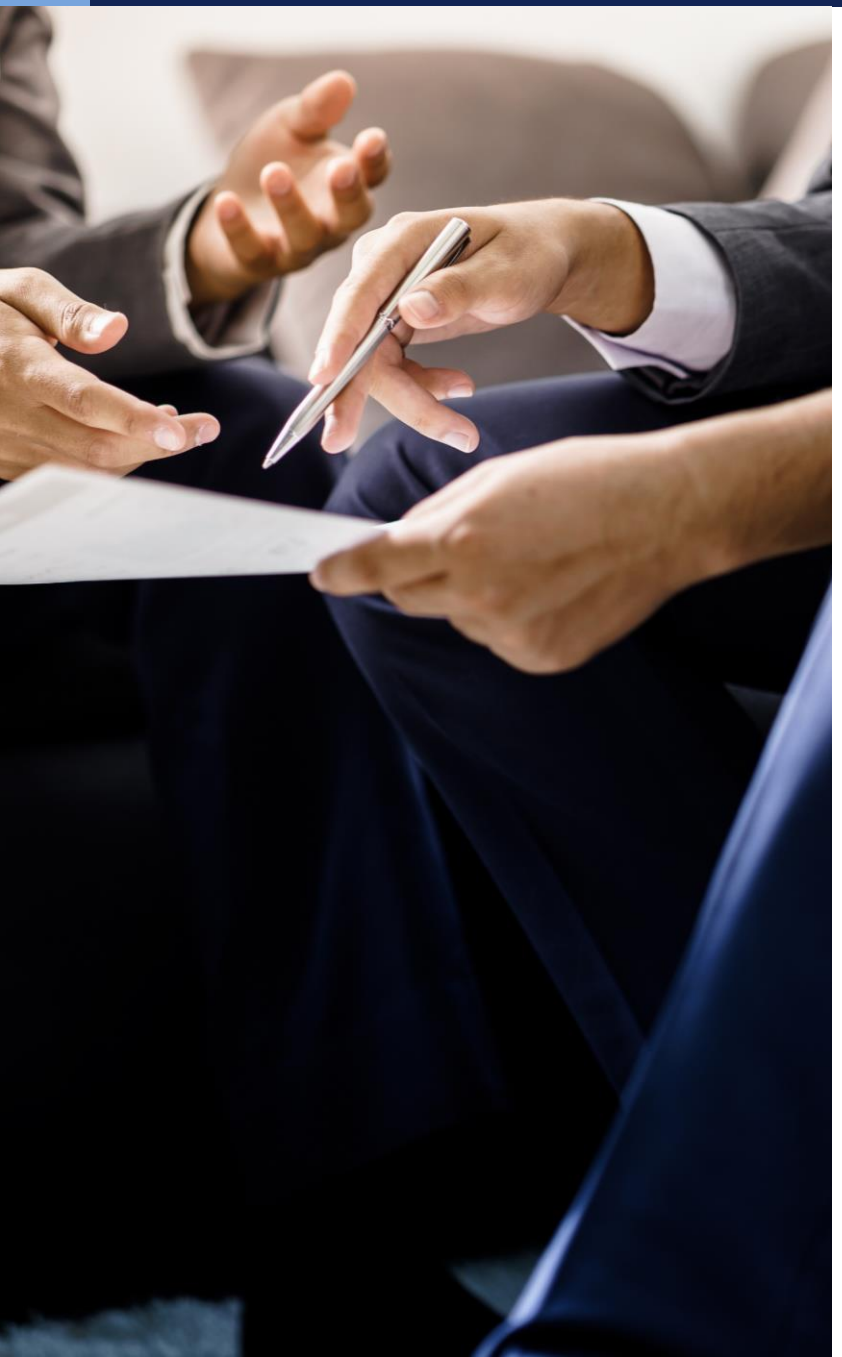
GDPR in 3 words – The Three Cs



Compliance

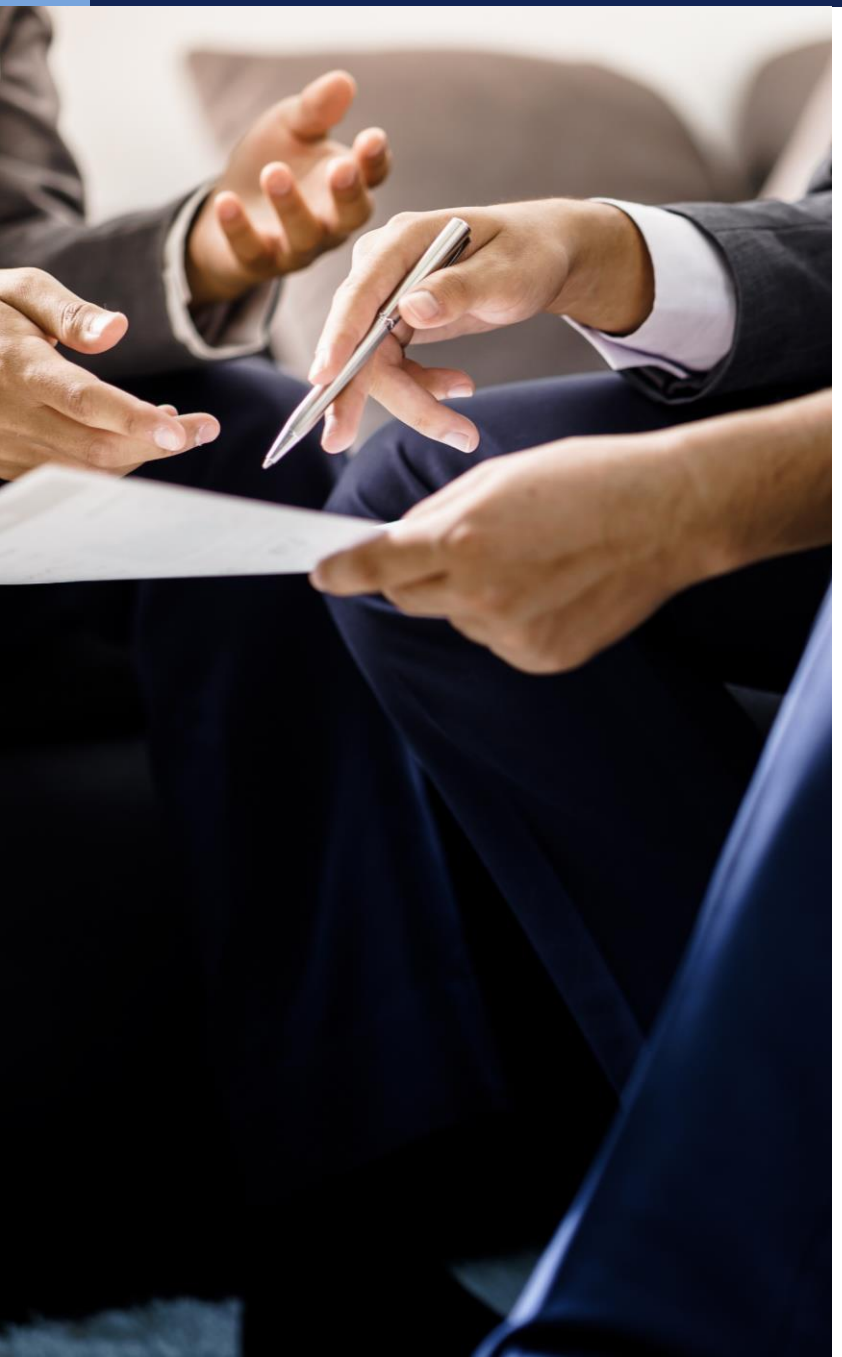
Consent

Communication



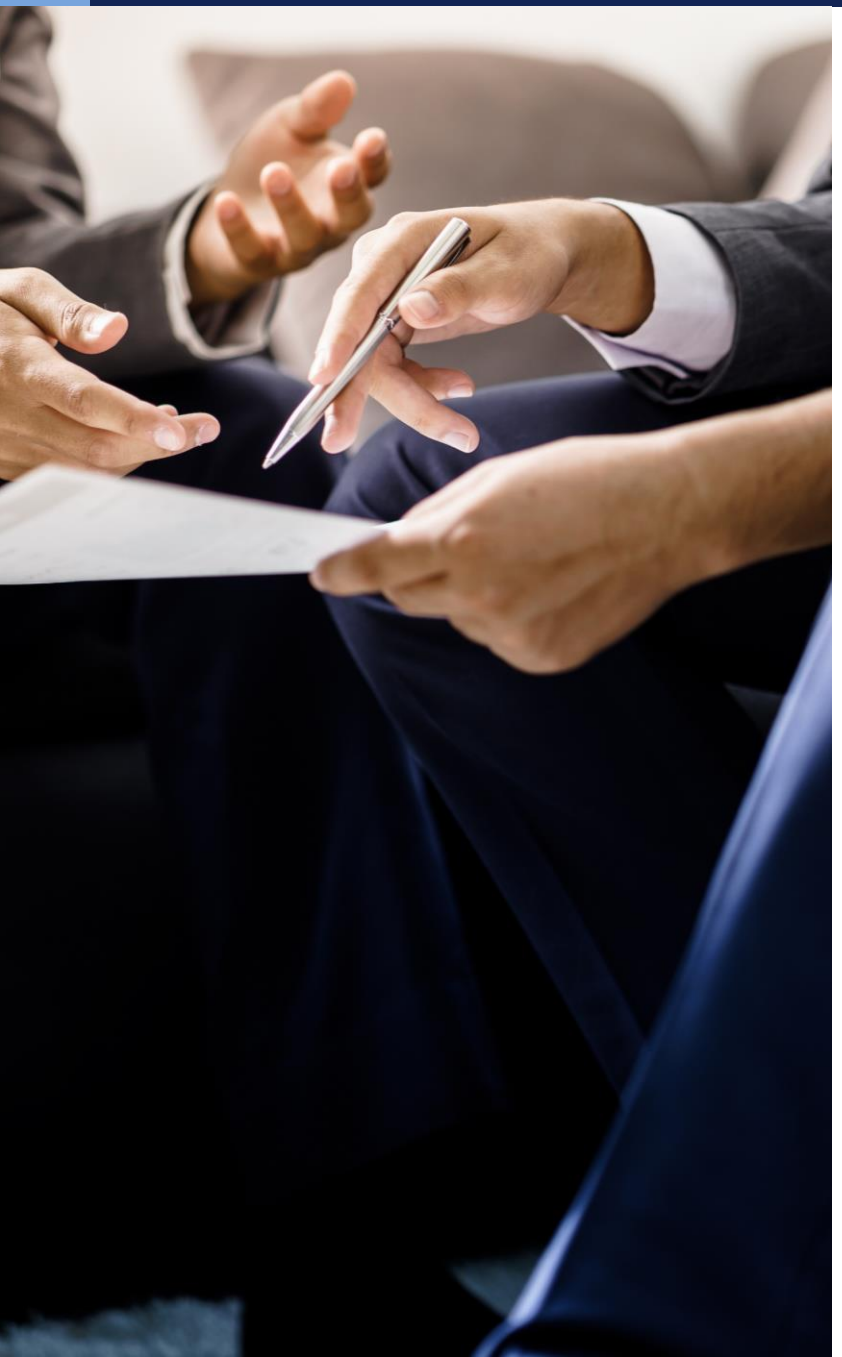
Rights to Access

- Under the GDPR, individuals will have the right to obtain:
  - confirmation that their data is being processed;
  - access to their personal data; and
  - other supplementary information including:
    - purposes
    - categories
    - recipients
    - retention periods
    - data sources
    - automated decision making and profiling
  - compliance is more strict and timely
- Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer



Right to be Informed

- The information you supply about the processing of personal data must be:
  - concise, transparent, intelligible and easily accessible;
  - written in clear and plain language; and
  - free of charge (previously you could charge a fee)
- The individual must be informed at the time of obtaining data directly from them or within a reasonable period (a month) in the case of data obtained from other sources; or
- If the data are used to communicate with the individual, at the latest, when the first communication takes place



Communication

- Has to be:
  - aligned with the individual's Right to be Informed
  - concise, transparent, intelligible, easily accessible and free;
  - in line with process for data breaches

What do you need to do right now?

1. **Awareness** - you should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR.
2. **Information you hold -** you should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit, across the organisation, or within particular business areas.
3. **Communicating privacy information -** you should review your current privacy notices and put a plan in place.
4. **Individuals' rights -** you should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.
5. **Subject access requests -** you should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.
6. **Processing software -** you should review your applications and tools to ensure that your systems, access rights and documentation processes are adequate for compliance.

What do you need to do right now?

7. **Legal basis for processing personal data** - you should look at the various types of data processing you carry out, identify your legal basis for carrying it out and document it.
8. **Consent** - you should review how you are seeking, obtaining and recording consent and whether you need to make any changes.
9. **Data breaches** - you should make sure you have the right procedures in place to detect, report and investigate a personal data breach.
10. **Data Protection by Design and Data Protection Impact Assessments** - you should familiarise yourself now with the guidance the ICO has produced on Privacy Impact Assessments (PIAs) and work out how to implement them in your organisation.
11. **Data Protection Officers** - you should designate a Data Protection Officer, if required, or someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements.
12. **International** - if your organisation operates internationally, you should determine which data protection supervisory authority you come under.

Questions

Q. Are there rules around parsing from LinkedIn when not personally connected to the individual?

- LinkedIn profiles are published under a user agreement and privacy policy between the user and LinkedIn. This does not automatically flow to anyone using the service.
- Whether you are connected to an individual or not, you have the ability but not the right to view a profile. You don't have an automatic right to take that data and process it.
- Under GDPR we believe you will strictly need consent and to inform the candidates whose data you are processing. In reality, you need to consider the degree of risk and likelihood of a candidate taking umbrage.
- The lawful basis of 'legitimate interest' could be used as a justification but under GDPR this is strengthened to protect the individual and the Controller must demonstrate "compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject".

Q. What are the rules around holding candidate data prior to contacting them?

- Under GDPR the strict interpretation is that you need to inform a candidate what you are doing with their data at the time of gathering the data from them or within a reasonable (likely 30 days) period if from another source.
- There is a potential to research within a reasonable period and filter out candidates. In most cases, if you are going forward with someone then you would want to contact them before submitting their details to ensure they are a viable candidate. And that would comply with GDPR. The key will be tracking and keeping appropriate records.
- If you are reviewing, assessing and essentially processing data on candidates that you do not proceed with then you would need to consider how much holding and processing that data constitutes a risk if the candidate were to request access or make a complaint of non-compliance. That risk will to a large extent depend on the damage and disadvantage to the candidate and any restriction to their rights and freedoms.
- The longer you hold or process data without consent or informing, the greater the potential risk.

Q. What impact will GDPR have on companies based outside the EU?

- The GDPR is focussed on the rights and freedoms of EU citizens. If you are processing data on, or providing goods or services to, EU citizens, then you will need to comply, regardless of your location.
- If you are outside the EU and you have no interest in dealing with EU citizens, and you have the systems and processes by which you can validate that the personal data you hold or process does not relate to EU citizens then you should have limited risk.
- There is a wider question as to how the EU would actually enforce compliance or apply penalties to companies in locations outside the EU.

Q. What impact will Brexit have on GDPR?

- The UK Government has committed to complying with GDPR by 25 May 2018, under the same timescales as the EU.
- A whitepaper was published on 2nd Feb 2017, confirming that the UK Government intended to continue this commitment to compliance for personal data transfers between the UK and EU.
- So, Brexit makes no real difference assuming that post Brexit, the UK having implemented the GDPR will be deemed an adequate jurisdiction for Data Privacy.

Q. How will GDPR be enforced?

- The EU Commission will increase the powers of Supervisory Authorities (SAs), the local geographic data protection bodies.
- These will include investigative powers (audits, reviews, notifications) and supervisory powers (warnings, compliance orders, fines).
- These will be supported and underpinned by the rule of European Law.
- Member States will have individual discretion to decide the rules on criminal sanctions for infringements of the GDPR.