HARNEYS

Start-up smart: GDPR compliance made easy

The key elements of the European General Data Protection Regulation (***GDPR***) for start-up businesses to consider include:

Will the GDPR apply to you? Broadly speaking, the GDPR applies to all entities processing personal data of data subjects residing in the EU, regardless of the entity's location. Follow our Flowchart to find out more.	**What is "personal data"?** Personal data is any information relating to an identified or identifiable individual. For example, names, email addresses, online identifiers (like IP addresses), and location data.
When is it lawful to process personal data? Processing should have a lawful basis (eg consent, contract, or legal obligation). It must be transparent – you must tell an individual why and how you are processing their data.	**Understanding the purpose of processing** You must record the purpose of your processing. You cannot change the purpose the processing was intended for (unless you get consent or have a clear legal obligation).
Do we have to limit the data we hold? The data you process must be adequate, relevant, and **limited to what is necessary**. Keep the 'need to know' data, and remove the 'nice to have'!	**Ensuring the accuracy of personal data** You must take every reasonable step to ensure the personal data you hold is not incorrect or misleading.
How long can we keep data? Do not keep personal data longer than you need it. Determine, document, and adhere to retention periods for each type of data you hold.	**Implementing Confidentiality and Security** You must have appropriate security measures in place to protect against the loss, destruction, or damage of personal data.
Are we accountable? Controllers of personal data must take responsibility for personal data. You must be able to demonstrate compliance with the GDPR.	**What are the rights of individuals?** Individuals have various rights, including the right of access to their data, erasure (often called a "right to be forgotten"), and to object to processing, etc.
Who we do notify in the event of a breach? Data breaches must be reported within 72 hours. In some circumstances, this is to the local data authority and the individual concerned.	**Do we have to appoint a mandatory officer?** Data protection officers must be appointed by entities in some circumstances, to independently and expertly monitor data protection compliance.
Can we conduct "automated processing"? Strict rules apply to automated decision-making, like profiling, including the right to object in certain circumstances.	**Applying Privacy by Design** Central to compliance is the integration of data protection from the outset of processing activities and business practices, from design and by default.

Elina Mantrali
+357 99 516189
elina.mantrali@harneys.com
Cyprus

Charlotte Allery
+1 284 852 4374
charlotte.allery@harneys.com
British Virgin Islands