GDPR QUICK GUIDE
FOR DATA PROCESSORS

The EU's General Data Protection Regulation ('GDPR') dramatically increases potential penalties for failing to properly protect customer data, and introduces new responsibilities and liability for firms who act as data processors. As a result, data processing businesses need to urgently prepare for it.

WHAT YOU NEED TO KNOW

- The GDPR takes effect on 25th May 2018.
- Unlike the current Data Protection Principles, it applies not just to data controllers (i.e. business who collect customer data and determine how that data is used), but also data processors (i.e. firms who handle or process data on behalf of data controllers).
- Data controllers are obliged to ensure that their expectation in relation to data protection and associated liability is built into their contracts with data processors.
- The GDPR introduces a duty on all organisations including data processors to report certain types of personal data breach.
- You may be obliged to appoint a Data Protection Officer.

WHAT IT MEANS FOR DATA PROCESSORS

The GDPR puts significant focus on outsourced data handling and processing activities, which means you should expect increased scrutiny from customers and regulators about the data security measures you have in place, including requests for information about your data security and data protection procedures.

You'll need to have a plan in place for urgently assessing, responding to and reporting data breaches, as well as agree on the process for notification in the event of a breach that relates to personal data you handle on behalf of a data controller.

Expect to receive requests from your customers to revise existing contracts, or sign new contracts, covering the new GDPR requirements, as they are required to have in place explicit contractual obligations when they outsource data processing activities to third parties.

If you use sub-processors or contractors for any part of your data processing activities, they should comply with your contractual data protection obligations, as you will be liable. If any of your sub-processors or contractors are located outside the EU, consider if you are able to transfer personal data to them without a specific legal basis, or specific agreement from your customers.

Finally, the GDPR singles out certain groups (minors) and certain types of data (special category data, including health and biometrics data) for specific attention. If you process children's data, or any special category data, you will be under enhanced processing obligations when the GDPR comes into effect.

WHAT YOU SHOULD DO

- Map and record your data processing activities.
- Make sure you are ready to respond to due diligence requests from your customers.
- Have a data breach response plan in place, and agree with your data controllers who will notify the UK Information Commissioner's Office (ICO) in the event you suffer a reportable data breach.
- Be prepared for requests to amend your existing contracts to explicitly cover your data processing activities, and what liability you assume for these.

FOR MORE INFORMATION

For more information on the GDPR, you can view the full guide on the ICO website:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

If you'd like to speak to someone from CFC about anything related to the GDPR, email us at gdpr@cfcunderwriting.com