DATA PROTECTION & CYBER SECURITY – THREATS TO CONSIDER WHEN EXPANDING YOUR BUSINESS

Viktoria Protokova
Moderator
CHARLES RUSSELL SPEECHLYS LLP
London, England
viktoria.protokova@crsblaw.com

Afra Mantoni
UGHI AND NUNZIANTE LAW FIRM
Milan, Italy
amantoni@unlaw.it

Donna Wilson
MANATT, PHELPS & PHILLIPS, LLP
San Francisco, California, USA
dlwilson@manatt.com
If your client is planning to acquire a business in the EU, it is advisable to ask relevant data protection due diligence questions. Below are the key questions that you and your clients should ask the target when running a corporate due diligence on the deals that contain personal consumer/employee data.

- Does the target provide its employees, customers or other individuals with a privacy policy? Note: Request for a copy of such policy and ask to clarify how such policies are communicated (e.g. website/link/employee handbook/employment agreement).
- Does the target keep personal data updated and accurate? Ask to describe the method on how it’s done.
- Does the target have the procedures/policies in place to deal with data protection rights, including subject access requests?
- Does the target have certified its information security measures (e.g. ISO, BSI)? Request a copy of such certifications.
- Inquire what IT measures the target has in place to protect personal data in transit and at rest (e.g. encryption, restricting portable devises connectivity).
- Does the target allow the remote access to its network and/or data (via Citrix or blackberries)? Ask to describe what the rules around remote access are.
- Does the target ever been subject to hacking, infiltration, etc? If so, ask to please describe how it was handled.
- Request to provide evidence on how the targets’ employees/contractors are trained on data protection.
- Does the target use any third party organisations to obtain, record, store, destroy or organise any of the personal data. Request to provide the relevant agreements (examples of outsourcing may include: payroll processing, marketing outsourcing, HR management outsourcing, cloud outsourcing, expenses management, data centres or other BPO outsourcing).
- Does the target ever been investigated by a DPA due to an individual’s complaint with regards to its Data Protection compliance? If so, ask to describe the specific circumstances, including any results, enforcement action, undertaking, legal proceedings or criminal action.
- Has the target ever been audited by a DPA?
- Have the targets’ employees ever been found guilty of offences relating to the exploitation of personal data. If so please describe it.
WHAT BUSINESSES NEED TO KNOW ABOUT THE EU PROPOSED GENERAL DATA PROTECTION REGULATION

The European Council (the Council) published its text of the proposed general data protection Regulation (the Regulation) on 15 June 2015. Negotiations have now commenced between the European Commission, the European Parliament and the Council. We expect agreement to be reached, and the final text published, during late 2015 / early 2016 with a two year implementation period.

- The Regulation not only applies to organisations located within the EU but it will also apply to organisations located outside of the EU if they offer goods or services to, or monitor the behaviour of, EU data subjects.
- The Regulation will make it easier for data controllers to rely on ‘legitimate business interests’ as a lawful ground to process personal data where there is a relevant and appropriate connection between the data controller and the data subject.
- Data processing agreements between data controllers and data processors will be required to contain extensive mandatory data protection clauses; for example controllers’ right to audit its processors and obligations on processors to assist with subject access requests and personal data breaches.
- Member states may provide for additional special conditions for the processing of personal data for specific sectors and for the processing of special categories of data.
- Codes of Conduct and Certifications will be developed to assist data controllers and processors demonstrate their compliance with the Regulation and also as a means to legitimise international data transfers.
- Multinationals will benefit from a one stop shop, where the data protection authority in the member state where the controller or processor has their main establishment will be the lead authority in relation to data processing undertaken by that controller or processor.
- Organisations may, or where required by applicable member state law, appoint a Data Protection Officer.
- Data controllers and processors will be required to maintain a record of all of their data processing activities which must be made available for inspection.
- Serious data breaches must be notified to the DPA, in most cases within 72 hours. Data breaches may also need to be notified to the affected individuals who may have the right to claim compensation.
- The application for Binding Corporate Rules as a means to transfer personal data intra-group will be simplified.
- Fines of up to 2% of annual worldwide turnover of the preceding annual year or EUR 1million may be imposed for non-compliance. DPAs will also have the power to carry out data protection audits.