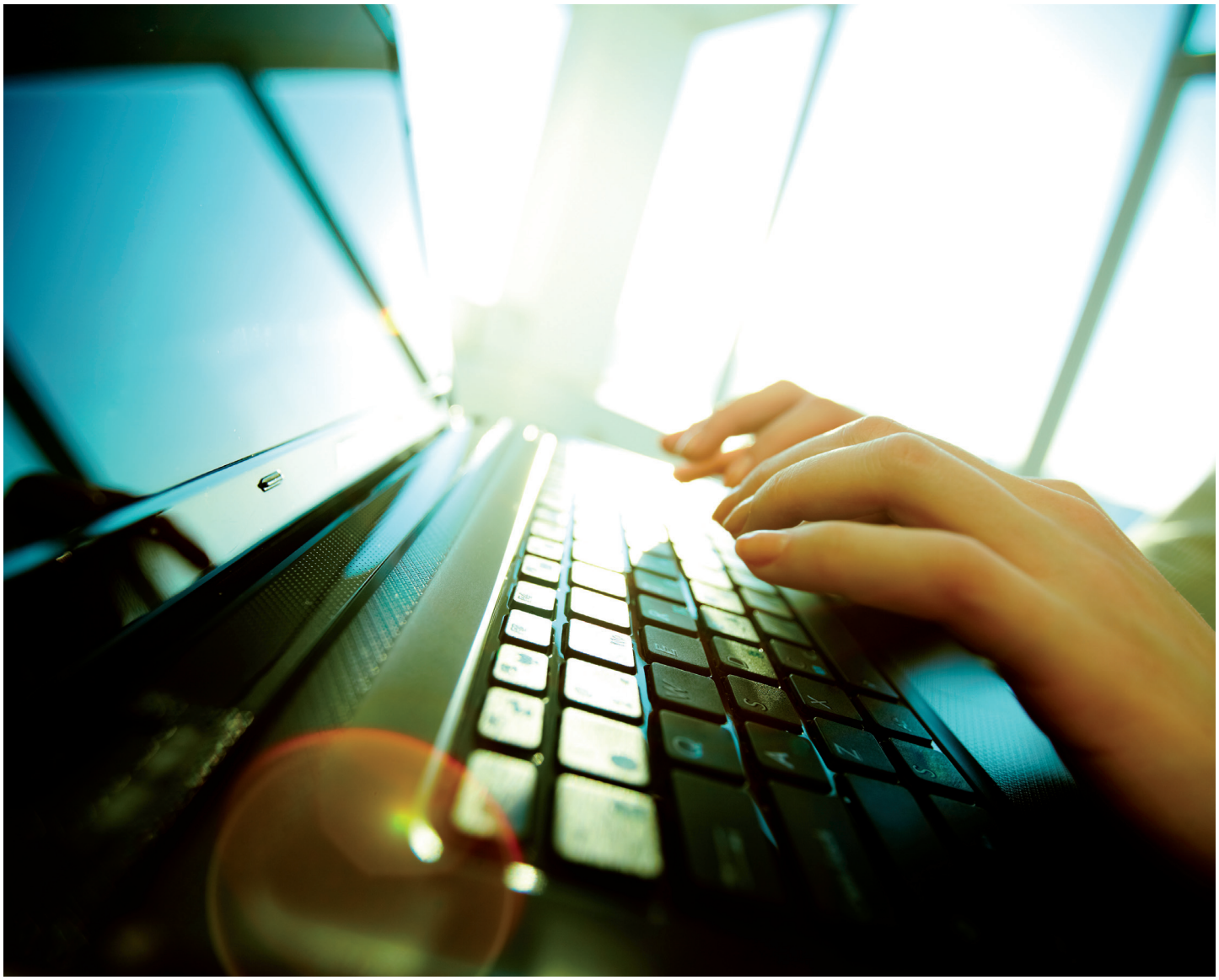
iGLOBAL LAW™
GLOBAL LABOUR LAW

iGlobal Strategic Guidance Series 2: Employee Compliance

(1) EU General Data Protection Regulation (GDPR)



A great deal has been written already about the EU GDPR. Many companies believe that lawyers and other related vendors are creating a climate of compliance fear for their own ends. We couldn't possibly comment.

iGlobal believes that while compliance with GDPR is important, for many if not most companies, it should be relatively straight forward and inexpensive. The effort and cost of compliance will depend on your size, your sector and your customer base/relationship.

For instance, a pan European business in an unregulated sector (such as IT) providing products or services only B2B should have significantly less to do and spend on GDPR than the same sized business in a regulated sector (such as financial services) providing B2C services and products.

The key is to do what you must do and no more

We set out below how best to approach an EU wide GDPR compliance programme.

The Essence of GDPR

GDPR applies equally to all EU states (including the UK despite Brexit). It comes into direct force automatically in all EU countries on May 25, 2018 and replaces the patchwork of data protection rules that currently exists across the EU.

Its core is your ability to '**demonstrate**' that you have complied with the rules. You are to be 'accountable' for your own data privacy. Your compliance must be actual not theoretical. You will no longer be required to register with the local data protection authority.

How to demonstrate compliance

You will be able to demonstrate your compliance by a combination of:

- Showing senior management commitment and involvement
- Documenting your data privacy policies and processes
- Taking steps to embed your policies and processing in your organisation
- Allocating data privacy responsibility clearly and openly
- Training of all relevant staff on data privacy
- Checking regularly that you are complying with your own policies and processes
- Feeding back into your policies and processes the results of your checks and training

How to Approach a GDPR Compliance Project

Step 1: Finding the facts: this will depend on what type of business you are.

For an unregulated B2B operating in one or more EU countries and processing relatively low levels of personal data you will need to gather the following information for a review:

- What type of personal data (including sensitive personal data) do you collect on your (1) employees; (2) customers and (3) anyone else?
- What is the approximate data volume, i.e. how many people (data subjects) do you have data on?
- How, when and where do you collect data?
- What international data transfers do you make (from and to which countries)?
- How do you keep secure, keep accurate and delete data when no longer needed?
- Who is responsible for data privacy in your organisation and where are they located?
- Which 3rd parties do you use to store or process data on your behalf, what data do they process and where do they process it?
- What is the status of the IT systems (yours and your suppliers) used to process your data?

If you are a regulated business, operating B2C or processing high volumes of data, in addition to all of the above you will need:

- To know and apply the relevant data privacy regulations for your sector
- To take a much closer and more detailed look at your data handling processes and IT framework to be sure that you will be compliant in 2018

Once you have collected and analysed this information you will be in a position to plan the most efficient compliance programme – everything you need to do but nothing that is unnecessary. Without first gathering in and analysing the information you risk either doing too much or too little.

Step 2: Planning your approach

We focus below on the approach for an unregulated B2B business that is not handling large volumes of data. As with Step 1, if you are a regulated or a B2C business or you are handling large volumes of data the approach below will be a good starting point but may not be sufficient.

Mapping: From the Step 1 fact find:

- Map all your data flows, from collection point to deletion
- Identify the nature of the data collected (personal or sensitive personal)
- Identify the purpose for which the data is collected
- Identify the communication points – what are you telling people at the point of data collection
- What data subject consents do you currently get; how and when?

Designing: Design your overall compliance framework or 'Privacy Governance Structure':

- Who is to be in overall charge?
- Who is to be responsible day to day?
- Who has sign off on third party contracts involving personal data?
- What are the reporting lines?
- Who needs what training and how is it to be done?
- How is the Structure to be communicated internally?
- Do you need an EU Representative or a Data Protection Officer (see below)?

Embedding: Embed your data protection approach into your organisation:

- Draft or update your privacy policy documentation to reflect your decided approach (see below)
- Establish and document a continuous training programme for relevant stakeholders
- Document a process for impact risk assessments – how and when you will conduct them and how you will implement changes
- Decide on and incorporate data protection mechanisms into the technical specifications of your IT systems, networks, processing operations and business practices

Checking and revising: Establish a continuous review of your data privacy processes:

- Document how you will test/audit your own compliance and implement any changes needed

Step 3: Implementation questions

Do you need an EU Representative? Only if your data controllers or data processors for EU personal data are not located in the EU.

Do you need a Data Protection Officer? Only if you conduct regular and systematic monitoring of EU data subjects on a large scale or conduct large-scale processing of sensitive personal data (excluding the personal data of your EU employees).

What should be covered in the core data privacy policies and processes?

- Your Privacy Governance Structure
- What personal and sensitive personal data you will collect
- The legal basis for your collecting and processing that data
- How and when you will collect the data
- How and when you will communicate to data subjects the reason for holding the data, how it will be held and maintained and the data subjects rights in relation to the data (e.g. the right to know what is held, why it is held and to require its amendment or deletion)
- How and when you will seek the data subject's consent to the holding and use of the data (note that employee consent won't be considered as valid)
- How you will maintain the quality and security of the data
- How you will manage/report security breaches
- How (through training, monitoring, testing and auditing) you will make sure your policies are complied with at all levels on a day to day basis
- How and when you will carry out impact risk assessments
- What international data transfers you will carry out and why
- What will be the legal basis for making those international transfers and what steps you will take to ensure compliance

What other documentation should be available?

- Consent forms for non-employee personal data
- Compliance logs/records/inventory (covering all data processes undertaken, consents obtained, training undertaken, checks and audits carried out)
- Checklist of essential clauses for third party data processing contracts - often vendors use their own terms but you must make sure they are appropriate and compliant

What other documentation may need review?

- Employment offer and contract
- Communications Systems Policy

- Website Privacy Notice and Cookies Policy
- Whistleblowing Policy
- Compliance Hotline Policy
- Pension Form (if applicable)
- CCTV signage (if applicable)
- Subject Access Request response and process
- Data rectification/deletion response and process

What is lawful data processing?

You can hold/process personal data for a stated use if (amongst others):

- you have the valid consent of the data subject (not possible for employees)
- it is necessary for performing a contract with the data subject
- it is necessary to pursue your legitimate interests provided they don't clash with those of the data subject or their fundamental right to privacy
- it is necessary for carrying out your rights in the field of employment law, social security, and social protection
- it protects the vital interests of the data subject when the data controller cannot obtain consent

Personal data is any data that relates to an identifiable person.

Sensitive personal data includes racial or ethnic origin; political opinions; religious or philosophical beliefs, trade union membership; genetic data; biometric data; health or sex life data; sexual orientation.

Rights of your data subjects:

- To know what, why and how their data is collected and processed
- To correct data errors, withdraw their consent to data processing and require data deletion

Your obligations to your data subjects

- Inform the data subject of the purpose of the data processing
- Use the data only for the stated purpose
- Inform the data subjects of their rights in relation to the data
- Keep the data safe, secure and accurate
- Delete the data when it is no longer needed for the stated purpose
- Transfer the data across borders only when you are legally permitted to do so

Countries where the GDPR will apply (all EU member states, including the UK)

Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK

iGlobal Law
71 Queen Victoria Street
London
EC4V 4AY

T: +44 (0) 20 7406 1639
E: info@igloballaw.com
www.igloballaw.com

We would welcome your feedback:
Please contact Karen Mosley
karen.mosley@igloballaw.com

Global labour and compliance law solutions for multi-national employers