A LITTLE BEE BOOK

“How it Works”
GDPR

This book belongs to:

_____

_____

_____

A LITTLE BEE BOOK

“How it Works”
GDPR

Adapted from a variety of sources by **Bob Yelland**

Notice: Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients’ business and any actions the clients may need to take to comply with such laws and regulations. The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting, or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.

To find out more visit **ibm.com/GDPR**

For more copies of this book, or to read others in the series, visit: **littlebeelibrary.com**

After four years of debate, the General Data Protection Regulation (GDPR) was ratified by the European Union during April 2016[1] and has now become law, although member states have a two-year period to implement into national law.

This means that companies will be expected to be fully compliant from **May 25th 2018**[2].

GDPR is designed to give individuals better control over their personal data and establish one single set of data protection rules across Europe.

Organisations outside the EU are subject to this regulation when they collect data concerning any EU citizen[3].

50% of global companies[4] say they will struggle to meet the rules set out by Europe unless they make significant changes to how they operate, and this may lead many companies to appoint a Data Protection Officer.

Personal data is defined as any information relating to an identified or identifiable natural person[5].

This includes online identifiers, such as IP addresses and cookies if they are capable of being linked back to the data subject.

This also includes indirect information, which might include physical, physiological, genetic, mental, economic, cultural or social identities that can be traced back to a specific individual.

There is no distinction between personal data about an individual in their private, public, or work roles – all are covered by this regulation.

There will potentially be a substantial increase in fines for organisations that do not comply with this new regulation[5].

Penalties can be levied up to the greater of ten million euros or two percent of global gross turnover[3] for violations of record-keeping, security, breach notification, and privacy impact assessment obligations.

These penalties may be doubled to twenty million euros or four percent of turnover, for violations related to legal justification for processing, lack of consent, data subject rights and cross-border data transfers[5].

Companies will be required to “implement appropriate technical and organisational measures”[3] in relation to the nature, scope, context and purposes of their handling and processing of personal data. Data protection safeguards must be designed into products and services from the earliest stages of development.

These safeguards must be appropriate to the degree of risk associated with the data held and might include:

- Pseudonymisation and/or encryption of personal data
- Ensuring the ongoing confidentiality, integrity, availability and resilience of systems
- Restoring the availability and access to data in a timely manner following a physical or technical incident
- Introducing a process for regularly testing, assessing, and evaluating the effectiveness of these systems

A key part of the regulation requires consent to be given by the individual whose data is held. Consent means “any freely-given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed”[6].

Organisations will need to be able to show how and when consent was obtained. This consent does not need to be explicitly given, it can be implied from his or her relationship with the company. However, the data obtained must be for specific, explicit and legitimate purposes.

Individuals must be able to withdraw consent at any time and have a right to be forgotten, if that data is no longer required for the reasons for which it was collected, and it must be erased.

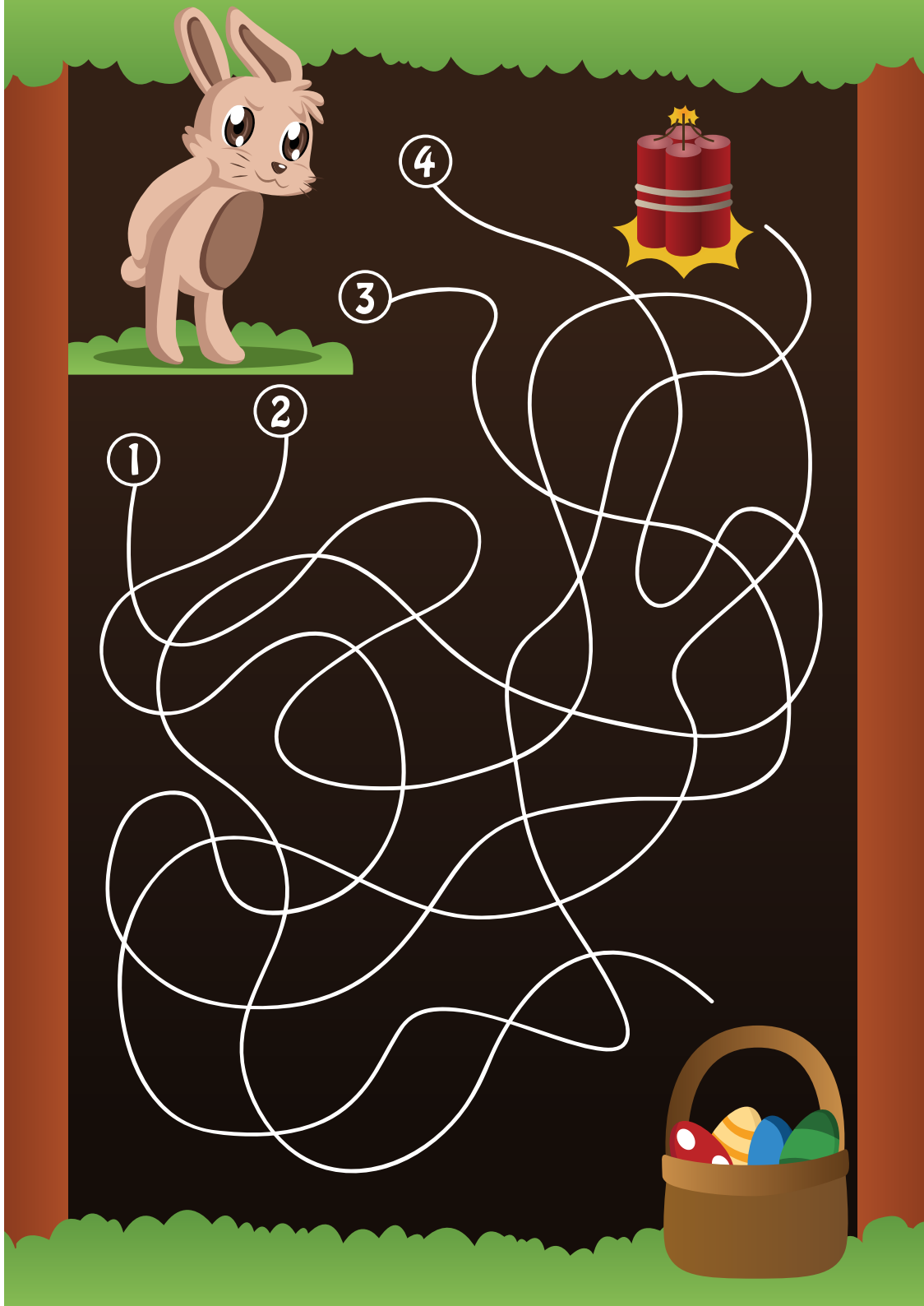
When companies obtain data from an individual, some of the areas that must be made clear to the data subject are:

- The identity and contact details of the organisation behind the data request
- The purpose of acquiring the data and how it will be used
- Whether the data will be transferred internationally
- The period for which the data will be stored
- The individual's right to access, rectify or erase the data
- The individual's right to withdraw consent at any time
- The individual's right to lodge a complaint

The regulations demand that individuals must have full access to information on how their data is processed and this information should be available in a clear and understandable way.

Individuals can make requests, and these must be executed “without undue delay and at the latest within one month of receipt of the request”[3].

Where requests to access data are manifestly unfounded or excessive then small and medium sized enterprises will be able to charge a fee for providing access.



Companies must report breaches of security "leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"[6].

In the event of a personal data breach, companies must notify the appropriate supervisory authority "without undue delay and, where feasible, not later than 72 hours after having become aware of it"[6] if the breach is likely to "result in a risk for the rights and freedoms of individuals".

During March 2016, the UK Information Commissioner's Office published[7] 'Preparing for the General Data Protection Regulation (GDPR) – 12 Steps to Take Now'. Some of these steps for organisations are summarised next.

1. Ensure key departments are aware that the law is changing, and to anticipate the impact of GDPR.
2. Document what personal data is held, where it came from and with whom it is shared.
3. Review current privacy notices and make any necessary changes.
4. Review procedures to address the new rights that individuals will have.
5. Plan how to handle requests within the new time frames and provide the required information.
6. Identify and document the legal basis for each type of data processing activity.
7. Review how consent is sought, obtained and recorded.
8. Make sure procedures are in place to detect, report and investigate data breaches.
9. Designate a Data Protection Officer to take responsibility for data protection compliance.

IBM offers a comprehensive approach to prepare for GDPR compliance with solutions and services from assessment to full-scale implementation. Our approach covers all necessary activities to support GDPR readiness across five domains: GDPR governance, employee training and communications, processes, data and security.

IBM Information Lifecycle Governance provides insight into all personal data and the tools and methodology to syndicate, instrument and enforce policies. IBM Security provides pervasive and intelligent internal and external network defences, incident response and security restrictions. Our Citizen Interaction Centre is pivotal in helping fulfil citizen GDPR rights and our Optim solution brings method, tools and state-of-the art technology to control and desensitise personal data.

Start your GDPR journey with IBM.

Sources:

(1) EU General Data Protection Regulation ratified: KPMG 2016
assets.kpmg.com/content/dam/kpmg/pdf/2016/05/EU-General-Data-Protection-Regulation-ratified-18-04-2016.pdf

(2) Guidance: what to expect and when: Information Commissioner's Office.
ico.org.uk/for-organisations/data-protection-reform/guidance-what-to-expect-and-when/

(3) Overview of the General Data Protection Regulation (GDPR): Information Commissioner's Office
ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

(4) Preparing for the EU GDPR: What You Need To Know: James Walker. SC Media 4th March 2016.
www.scmagazineuk.com/preparing-for-the-eu-gdpr-what-you-need-to-know/article/531492/

(5) A Summary of the EU General Data Protection Regulation: Peter Galdies DatalQ. 14th January 2016.
www.dataiq.co.uk/blog/summary-eu-general-data-protection-regulation

(6) EU Official Journal issue L 119
eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L:2016:119:FULL&from=EN

(7) Preparing for the General Data Protection Regulation (GDPR): 12 steps to take now. Information Commissioner's Office 14th March 2016.
ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf