HERZOG

HERZOG FOX & NEEMAN

The UK Data Protection Reform

Herzog's Guide to The Key Changes

June 2025

INTRODUCTION

The United Kingdom's parliament has approved the **Data (Use and Access) Bill**, which is now pending a Royal Assent, in order to become an act (the "**Act**").

In recent years, data protection in the UK has been regulated mainly by two laws: the Data Protection Act 2018 and the UK General Data Protection Regulation (together, "**UK Data Protection Laws**"), which were based on and aligned with the European Union's Geneal Data Protection Regulation.

Over the years, the UK Government has decided to depart from the EU-based regulatory regime. According to the presented reform, some elements of the current UK Data Protection Laws create barriers, uncertainty and unnecessary burdens for businesses and consumers. The Act is intended to update and streamline the requirements of the current legislation, and to reduce burdens on organization while maintaining high data protection standards. Furthermore, the Act confers broad regulation-making powers on the Secretary of State exercisable in consultation with the Information Commissioner's Office (which will be replaced, under the Act, with the Information Commission. For ease of reference, in this document we will refer to the regulatory body as "ICO") and other relevant stakeholders, as well as various enforcement powers on the ICO in relation to key provisions. These powers are intended to support the ongoing refinement and evolution of the legal framework in the future.

Additionally, the Act amends the Privacy and Electronic Communications Regulations 2003 (the "**PEC Regulations**"), which were also based on the EU's regulatory regime in relation to the usage of tracking technologies such as **cookies** and to unsolicited **direct marketing** communications. It further amends various other pieces of legislation with the aim of updating and expanding data-handling provisions beyond the direct context of business-related data processing.

Failing to comply with the provisions of UK Data Protection Laws can result in administrative fines of up to **£17,500,000 or up to 4% of the total worldwide annual turnover**, whichever is higher. In addition, under the PEC Regulations, the ICO can impose fines of up to **£500,000**.

Most of the Act's provisions will come into force on a **date to be determined in regulations**, while certain provisions such as those relating to the ICO's enforcement powers and certain amendments to the right of access will take effect within up to two months of the Acts' commencement.

Companies that are subject to UK Data Protection Laws and have implemented the applicable requirements in their data processing activities should review their practices, procedures and policies, and adjust them to meet the Act's updated requirements.

To assist with understanding the updated requirements under the Act, we are pleased to present this playbook, which provides a general overview of **key changes presented by the Act** and the **practical steps** that companies should take in order to comply with them. In addition, we highlight some additional changes made by the Act that do not require significant changes in the related procedures and processors, but provide further regulatory clarity on the respective subject matters. The focus of the playbook will be on the **changes most relevant to businesses handling personal data as part of their everyday activity**.

GENERAL PRINCIPLES

Lawfulness of Processing

What Has Changed?

The Act introduces a new lawful ground to be relied on when processing personal data: **Recognized Legitimate Interest.**

The Act sets forth **specific and limited conditions** for processing which could be based on Recognized Legitimate Interest, for example disclosing personal data to a third party for the performance of a **task carried out in the public interest**, processing which is necessary for national security, for responding to **an emergency**, or processing personal data for **public security or defense.**

What Should You Do?

Companies should **review** their current lawful grounds for processing personal data and **assess** whether they may rely on the new lawful grounds that better fit their processing operations and purposes.

Changing the lawful grounds for processing **must also be reflected in the privacy policy.**

GENERAL PRINCIPLES

Automated Decision-Making

What Has Changed?

Under the UK Data Protection Laws, it is generally prohibited to make a decision that significantly affects a data subject's legal rights or similar important interests based solely on automated processing, including profiling, unless certain exemption apply.

The new Act introduces both **clarifications** and **amendments** to this framework.

First, the Act clarifies that: (i) a decision is based solely on automated processing **when there is no meaningful human involvement** in the taking of the decision (e.g., when the decision was reached mostly by means of profiling), and that: (ii) a "significant decision" shall be a decision producing **legal effect or other "similarly significant" effect** for the data subject.

Second, the Act **revises** the existing prohibition by generally allowing a significant, solely automated decision to be based entirely or partly on personal data, provided that the controller puts in place **the appropriate safeguards to protect data subject's rights, freedoms and legitimate interests.** The safeguards must consist of:

- providing the data subject with information about such decisions taken with respect to the data subject;
- enabling the data subject to make representations about such decisions;
- allowing the data subject to obtain human intervention in relation to such decisions; and
- allowing data subjects to contest such decisions.

In contrast to the foregoing, the Act stipulates that a stricter rule will continue to apply where a significant decision based solely on automated decision making is based on **special categories of data.**

Under current UK Data Protection Laws, such decision making is prohibited unless the data subject has given its **explicit consent**, or **it is necessary for the public interest** (as determined under applicable law).

The Act **further refines these conditions**, by requiring:

- the explicit consent of the data subject; **or**
- that such decision is: (i) necessary for public interest, **as well as** (ii) necessary for the performance of a contract **or** is made in accordance with a requirement/ authorization set by applicable law.

What Should You Do?

Companies that conduct data processing operations that are **solely** based on automated decision making, and produce significant decisions in reliance thereon, must implement **safeguards at least as stringent as outlined in the Act.**

Where such decisions are based on special categories of data, companies should **assess the current legal bases on which they rely**, and ensure such activities are in line with the additional requirements set by the Act.

GENERAL PRINCIPLES

Data Protection by Design

What Has Changed?

The Act introduces the concept of **'children's higher protection matters'**, reinforcing the principle of **'data protection by design and by default'** in the context of information society service (online services of a commercial nature, or "ISS"(targeted at children.

When implementing appropriate technical and organizational measures for the protection of personal data, controllers must now explicitly consider that **children require specific protection**, as they may be less aware of the risks, consequences, and safeguards associated with data processing. Moreover, controllers must account for the **diverse needs, developmental stages, and levels of maturity** across different age groups of children.

What Should You Do?

Companies falling within this scope should **reassess their existing data protection measures** by taking into account that children may require enhanced safeguards due to their limited understanding, evolving capacities, and increased vulnerability to harm.

GENERAL PRINCIPLES

Transfers of Personal Data

What Has Changed?

Under current UK Data Protection Laws, international data transfers are permitted where the recipient's jurisdiction is recognized by the Secretary of State as providing an adequate level of protection. In the absence of such recognition, transfers may be governed by appropriate safeguards, most notably of which is contractual arrangement stipulated in the UK Standard Contractual Clauses (also referred to as the 'UK Addendum').

The Act **enhances the Secretary of State's existing authority** to make regulations regarding the adequacy of third countries for personal data transfers from the UK. For example, the Secretary may now approve **all transfers** to a third country, **specific types of transfers**, or **transfers limited to certain sectors or geographic regions** within that country. The Act also introduces an **explicit obligation** for the Secretary to **monitor ongoing developments** in third countries, including any changes that could affect their level of data protection adequacy.

Additionally, the Act introduces a new requirement called the **'Data Protection Test'.** While based on existing adequacy principles, this test must now be **independently assessed by the transferring party** for each transfer relying on appropriate safeguards outside an adequacy decision. Meaning that **the test needs to be done in addition to implementing the applicable safeguards themselves.**

What Should You Do?

Companies should **review and update their international data transfer procedures to incorporate the new Data Protection Test** introduced by the Act. This includes revising any relevant Transfer Impact Assessments and updating corresponding provisions in the company's Data Processing Agreements to ensure alignment with the new requirements.

Further, companies should be aware that **existing UK adequacy decisions may be subject to modification** to reflect the Secretary of State's expanded powers under the Act. Organizations relying on such decisions should **monitor regulatory updates** and be prepared to adapt their transfer mechanisms accordingly.

DATA SUBJECTS' RIGHTS

Data Subjects' Requests

What Has Changed?

The UK Data Protection Laws allow controllers to refuse data subjects' requests or to charge fees to exercise such requests in cases of '**manifestly unfounded or excessive requests**'.

The Act further stipulates that, in the event of refusal, the controller must, without undue delay: (i) provide the data subject with **the reasons for the refusal,** and (ii) inform the data subject of its right to **lodge a complaint with the ICO**.

Additionally, according to the UK Data Protection Laws, controllers must answer data subject's request without undue delay, and in any event within one month of the receipt of the request.

Under the Act, the controller may respond to data subjects' requests **before the end of the 'applicable time period'**. The applicable time period means the period of **one month beginning upon the latest of**: the receipt of the request; the receipt of information the controller requested to verify the identity of the data subject; or when the fee for 'manifestly unfounded or excessive' requests is paid. This period **may be extended** by two further months where necessary due to the complexity of the request or the number of such requests.

What Should You Do?

Controllers should update their **data subjects request procedures** to reflect the updated **response timeframes** for a request, as required under the Act.

Additionally, controllers should **establish clear criteria for classifying requests** as unfounded or excessive, along with updating the data subject request procedures to incorporate **the appropriate responses and actions** in connection therewith.

DATA SUBJECTS' RIGHTS

Right of Access

What Has Changed?

UK Data Protection Laws regulate the right of data subjects to access personal data concerning them, which is processed by the controller.

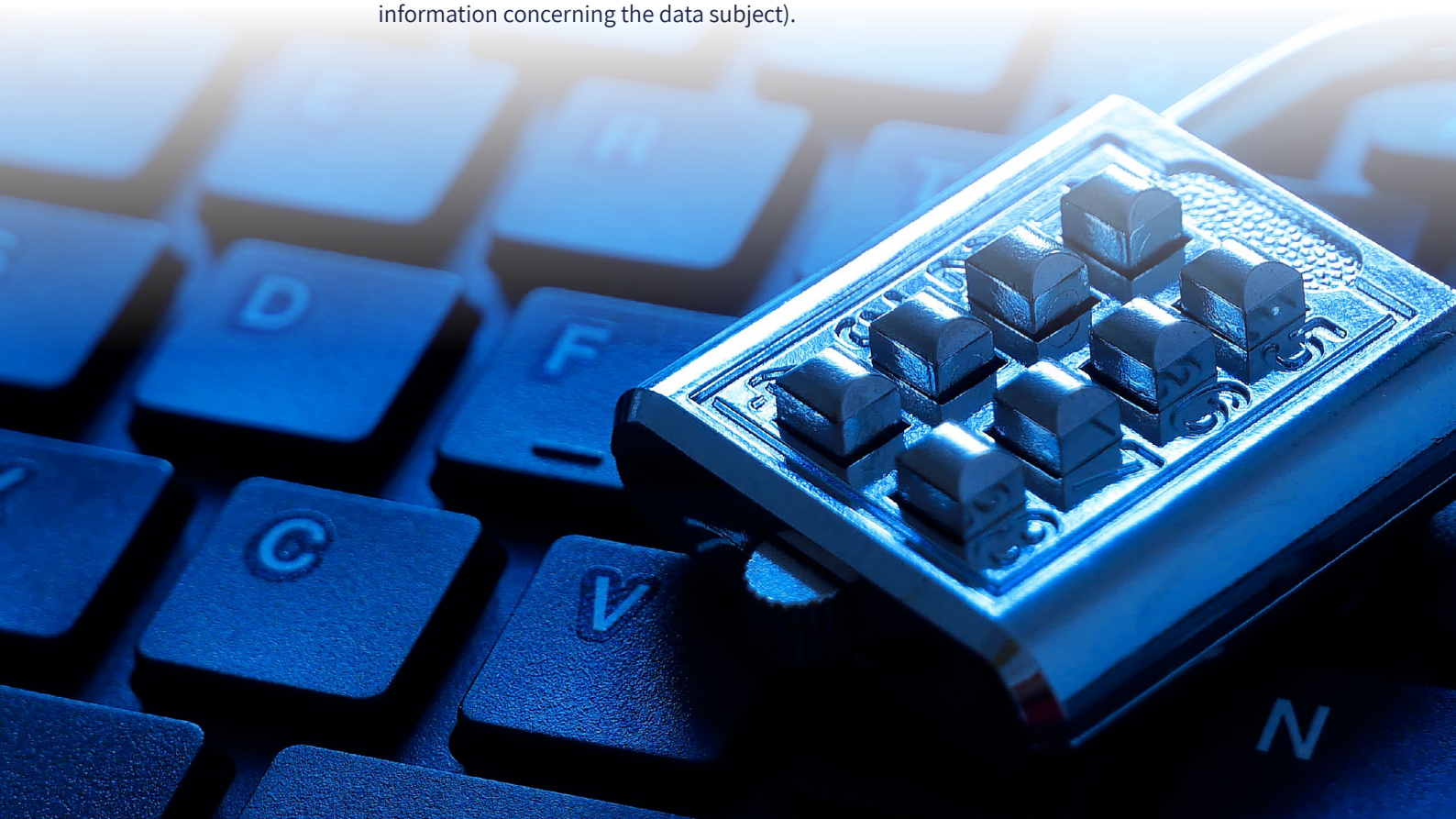
The Act stipulates the **scope** under which a controller should address a request to access, and determines that the data subject is only entitled to such confirmation, personal data and other information as **the controller is able to provide based on a reasonable and proportionate search for the personal data and other information requested.**

Under the Act, the controller may also require **further information** from the data subject in order to **identify the information or processing activities to which a request to access relates** (in cases where, for example, the controller processes a large amount on information concerning the data subject).

What Should You Do?

Controllers should review and potentially **update their data subjects request procedures** with respect to requests to access by:

- limiting their scope of response to only **what they are able to provide based on a reasonable and proportionate search** for the information requests;
- allowing them in certain cases to **require further information from the data subject** in order to identify the information or processing activities to which the request relates.



DATA SUBJECTS' RIGHTS

Data Subjects' Complaints

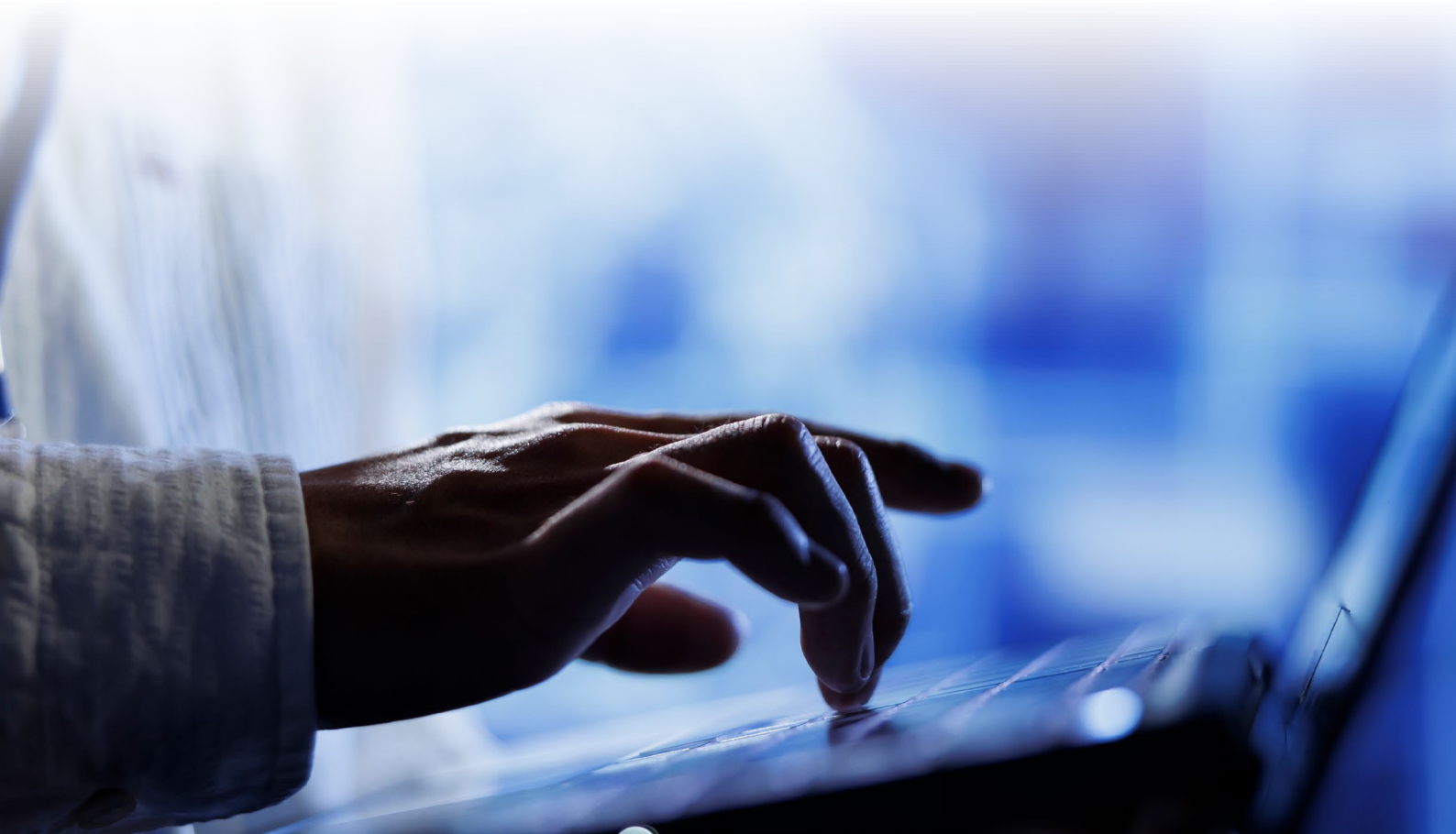
What Has Changed?

The Act introduces **a new complaint mechanism** that controllers are required to implement, enabling data subjects to submit complaints directly to the controller where they believe their data protection rights have been infringed.

This mechanism serves as a **catch-all right to help ensure that controllers uphold their data protection obligations.** As with other data subject rights, controllers are required to **acknowledge receipt** of the complaint, **investigate and address** the issue appropriately, and **keep the data subject informed** of the outcome. In addition, controllers must provide an **accessible and user-friendly complaint submission process**, such as a clearly visible online form.

What Should You Do?

Companies should **address the new complaint mechanism** both within their **internal data subject request procedures** and by **implementing appropriate tools** to ensure the complaints process is easily accessible to data subjects.



PRIVACY AND ELECTRONIC COMMUNICATIONS

Storing Cookies

What Has Changed?

The PEC Regulations, which are based on the EU ePrivacy Directive, prohibit organizations from storing information or gaining access to information stored in the terminal equipment of an individual, unless:

i. the individual is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; and the individual has given consent;

ii. where such actions are for the sole purpose of carrying out a transmission or communication, or

iii. where such actions are strictly necessary for the provision of the services (for example, the proper function of the website).

These rules apply to the placement of cookies and similar technologies (such as tracking pixels) on people's devices.

The Act reintroduces the 'strictly necessary' exemption, by providing a new, non-exhaustive list of illustartive examples for its application, which include purposes such as:

- The provision of an online service requested by the user - for example, in connection with information and security protection, fraud detection, correction of technical faults, user authentication, and maintaining records of the user's selections or the information provided to them.
- Collecting statistical information about how an organization's online service is used, with a view to making improvements to the service, provided that:
- (i) data is only shared with third parties assisting in the improvements; (ii) the purpose is disclosed to the user, and (iii) the user is given an opportunity to object.
- Enabling and enhancement of the appearance or functionality of an online service when displayed on a user's device, provided that: (i) the purpose is disclosed to the user, and (ii) the user is given an opportunity to object.
- Ascertaining the geographical position of an individual so that assistance can be provided in response to the individual's emergency communication from their device.

It is noteworthy that earlier drafts of the Act included the installation of software updates to ensure device security as an additional 'strictly necessary' purpose. The omission of this purpose in the final version may suggest that such a purpose cannot be presumed to qualify as 'strictly necessary'.

What Should You Do?

Companies should **re-assess their use of tracking technologies** in light of these clarifications to confirm whether existing exemptions remain applicable or whether new exemptions may now apply.

However, companies should take into account that each exemption **may impose alternative obligations** (such as providing users with the option to opt out, or informing them about these processes).

FURTHER CLARIFICATIONS

In the UK Data Protection Laws

Public Interest

Under current UK Data Protection Laws, the lawful basis of 'public interest' must be established by domestic legislation.

The Act expands on this principle by confirming that **'public interest' also includes international law, specifically the agreement between the UK and the US** on access to electronic data for the purpose of combating serious crime.

Additionally, the Act further clarifies the legal basis under UK Data Protection Laws for processing personal data in the performance of a task carried out in the public interest. It specifies that **the task must be that of the processing controller**, and another controller cannot rely on that same task as a lawful basis for its own processing.

The Information Commission

Data Protection Law designate the Information Commissioner as an independent official responsible for overseeing and enforcing the UK Data Protection Laws.

The Act **abolishes the Information Commissioner's Office and replaces it with a new 'Information Commission',** which assumes the statutory functions previously exercised by the Commissioner, with the current Commissioner transitioning to become the head of the new Commission, thereby transitioning from a single-commissioner model to a multi-member regulatory body.

Research and 'RAS' Purposes

Under current UK Data Protection Laws, 'research purposes' are to be interpreted broadly, encompassing activities such as technological development and mental health research. The Act further expands the definition of 'scientific research' to include **any research that can reasonably be regarded as scientific in nature and conducted in the public interest.**

The Act consolidates scientific research, historical research, and archiving purposes under a single term: '**RAS Purposes**'. These purposes are now expressly subject to specific safeguards and guiding principles designed to ensure the protection of personal data in these contexts.

Legitimate Interest

Under the current UK Data Protection Laws, processing is lawful if it is, inter alia, "*necessary for the purposes of the legitimate interests pursued by the controller or by a third party…*"

The Act sets out **non-exhaustive examples** of activities which may be in the legitimate interest of the data controller, including **direct marketing, intra-group transmission of personal data for internal administrative purposes, and ensuring the security of the network and the information systems.**

FURTHER CLARIFICATIONS

In the UK Data Protection Laws

Purpose Limitation (or Further Processing)

The Act sets out the conditions for determining whether the reuse of personal data ('further processing') is in compliance with the **purpose limitation principle** exists under UK Data Protection Laws.

This principle **prohibits further processing that is not compatible with the original purpose for which the personal data was collected.**

The Act clarifies that further processing would be compatible with the original purpose, inter alia, where -

- the data subject **consents** to the further processing, and the new purpose is specified, explicit and legitimate;
- the processing is carried out for the purpose of **scientific research or historical research, archiving in the public interest or statistical purposes;**
- the processing is carried out for the purposes of ensuring that it is processed in a manner compatible with the principles of processing (e.g., **purpose limitation, data minimization, accuracy,** etc.), or
- the processing is for **special purposes like the public interest, public security, responding to an emergency, protection of data subjects, complying with legal obligation of the controller** etc. Where the initial collection relied on the consent of the data subject, further processing for this purpose may only be allowed where it cannot be reasonably expected to obtain the data subject's consent for the new purpose.

Notification of a new purpose to the data subject is generally required, but may be exempted **in certain circumstances, including where providing such information is impossible or would involve a disproportionate effort.** The Act further sets out the relevant considerations to be considered and actions to be taken when determining whether this exemption applies.

FURTHER CLARIFICATIONS

In the PEC Regulations

Direct Communications by Charities

Under the current PEC Regulations, direct email communications are permitted only where: (i) the user has given explicit consent, or (ii) the contact details were obtained in the context of a sale or negotiations for a sale, the marketing relates to similar products or services, and the recipient was offered the opportunity to opt out.

The Act introduces a third exemption, allowing **charitable organizations to send email communications** where: (i) the purpose is to **further their charitable aims**; (ii) the recipient's details were collected in the context of **expressing interest in or support for** those aims, and (iii) the recipient was provided with **a simple means to refuse such communications**, either at the point of collection or with each message.

Reports on Data Breaches

Under the current PEC Regulations, a communications service provider was required to notify the ICO of any personal data breach 'without undue delay', a requirement the ICO (now to be replaced by the Information Commission) interpreted as within twenty-four hours. The Act clarifies this timeframe, extending the deadline to seventy-two hours from the point of becoming aware of the breach. Any delayed notification must include the reasons for the delay.

HERZOG'S TECHNOLOGY REGULATION DEPARTMENT

Herzog's Technology Regulation Department is a recognized market leader in its field.

The team is led by domain experts who possess a unique set of vital, **interdisciplinary** and **global** regulatory advisory skills, and are uniquely positioned to advise a range of clients, including leading multinational technology companies as well as start-ups and disruptive technologies vendors, on applicable regulatory and compliance considerations in numerous technological areas.

We understand that the **regulatory exposure** and scope of required **attention** of almost any company operating in the **digital and technological sphere** are much wider than one specific jurisdiction or legal discipline. As our clients are often on the forefront of this ever-evolving landscape, we further understand the impact of industry trends and compliance demands on our clients' businesses. Therefore, our team possesses in-depth knowledge of the increasing volume of regulations, enforcement actions, legislative and industry trends in a **myriad of jurisdictions, digital platforms** and leading **self-regulatory guidelines**. This enables our team to offer **practical, holistic** and **comprehensive** solutions for complex situations often presented by innovative technologies and disruptive business solutions, providing "hands-on" support to our clients on the strategic, corporate and operational aspects of their business, with the aim of mitigating our clients' legal and business risks.

Regulation of **personal information** has been dramatically expanding on a global basis. Companies processing data of hundreds of millions of data subjects as well as small start-ups - all are required to spend significant resources on understanding and implementing the constantly evolving legal challenges. Our Privacy & Data Protection team guides our clients on all matters relating to their data usage and assist them in navigating the numerous data protection regimes, in all the jurisdictions in which they operate.

HERZOG
HERZOG FOX & NEEMAN

The UK Data Protection Reform

Ariel Yosefi | Partner
Head of Technology Regulation
yosefia@herzoglaw.co.il

Ido Manor | Partner
Technology Regulation
manori@herzoglaw.co.il

Dan Shalev | Partner
Technology Regulation
shalevd@herzoglaw.co.il

Ruly Ber | Partner
Technology Regulation
berr@herzoglaw.co.il

Eden Lang | Partner
Technology Regulation
lange@herzoglaw.co.il

Dima Zalyalyeyev | Partner
Technology Regulation
zalyalyeyevd@herzoglaw.co.il

Or Noy | Associate
Technology Regulation
noyo@herzoglaw.co.il

On Dvori | Associate
Technology Regulation
dvorio@herzoglaw.co.il

Kevin David Gampel | Associate
Technology Regulation
gampelk@herzoglaw.co.il

Oded Kramer | Associate
Technology Regulation
kramero@herzoglaw.co.il

Zohar Malul | Associate
Technology Regulation
malulz@herzoglaw.co.il

Tal Habas | Associate
Technology Regulation
habast@herzoglaw.co.il

Benjamin (Ben) Reznik | Associate
Technology Regulation
reznikb@herzoglaw.co.il

Yonatan Glatt | Associate
Technology Regulation
glatty@herzoglaw.co.il

Adaya Ziv-Kisos | Associate
Technology Regulation
Zivkisosa@herzoglaw.co.il

Liron Adar | Associate
Technology Regulation
adarl@herzoglaw.co.il

Kobi Plotkin | Associate
Technology Regulation
plotkiny@herzoglaw.co.il

Eden Lapid | Associate
Technology Regulation
lapide@herzoglaw.co.il

Yuval Glazer | Intern
Technology Regulation
glezery@herzoglaw.co.il

Yuval Ram | Intern
Technology Regulation
ramy@herzoglaw.co.il

Gal Mechtinger | Intern
Technology Regulation
mechtingerg@herzoglaw.co.il

Yoel Toledano | Intern
Technology Regulation
toledanoyo@herzoglaw.co.il