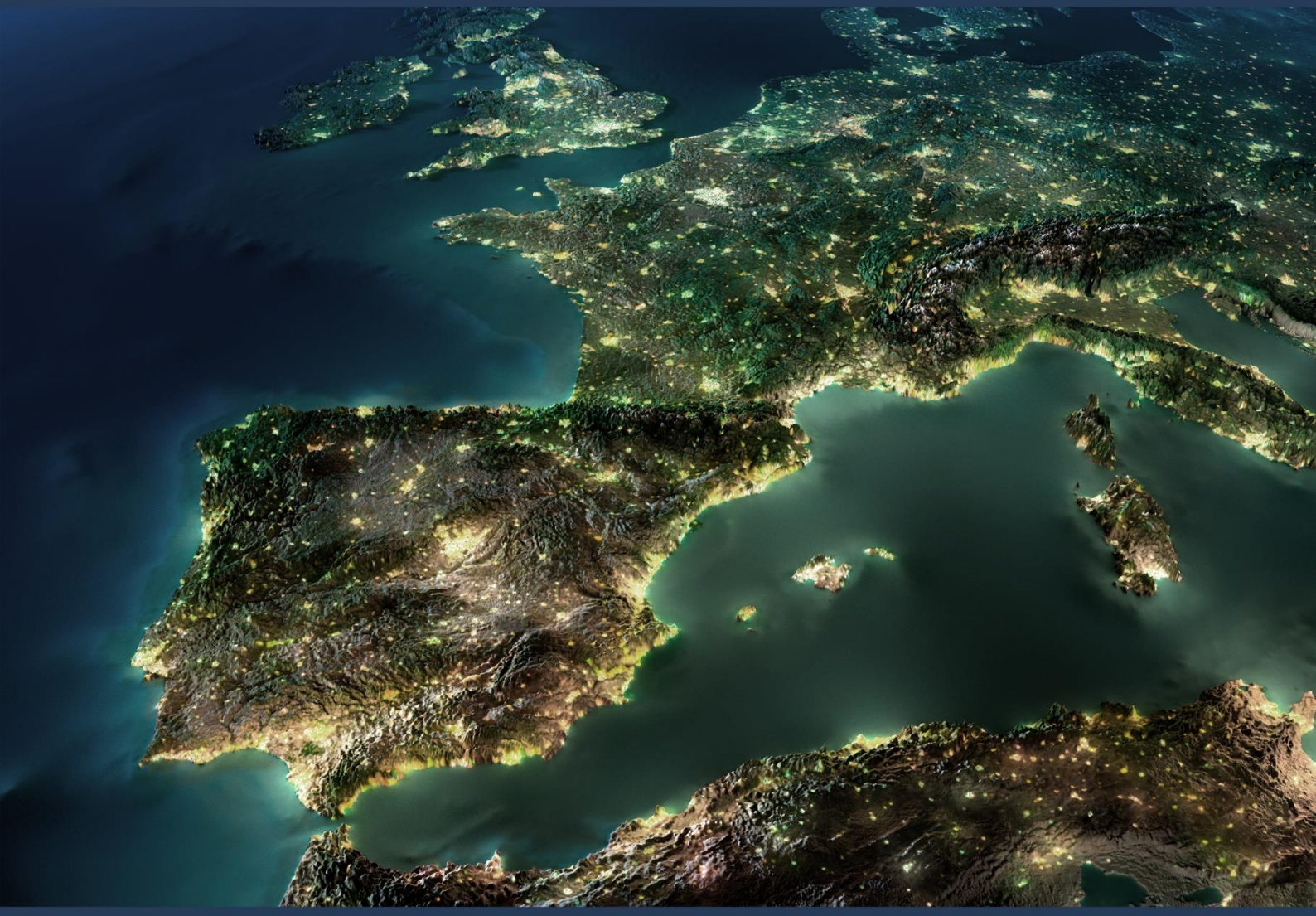
GDPR
Compliance Toolkit



Provided by: RS Risk Solutions Ltd

Blackgrove
Tandridge Lane
Lingfield RH7 6LW

01342 580106
www.rsrisk.solutions

TABLE OF CONTENTS

On 25 May 2018, the General Data Protection Regulation (GDPR) came into effect in the EU and across the United Kingdom. The GDPR replaces the Data Protection Act (DPA) and ushers in expanded rights to individuals and their data, placing greater obligations on businesses and other entities that process personal data.

The GDPR governs personal data, which it defines as any information that can be used to directly or indirectly identify an individual. This expansive definition includes the examples below, but this list is not comprehensive. If you're unsure whether something is personal data, the best practice is to treat it as such.

- Name and surname
- Home and email address
- Location data, such as a geolocator used by certain apps
- Online identifiers, such as a username
- Health information
- Income
- Cultural profile

What's New Under the GDPR?
Although the GDPR expands the definition of personal data from the DPA, many of the GDPR's main concepts and principles are the same as those in the DPA. However, there are new elements and significant enhancements. One of the most consequential of these revisions is how to handle personal data, which is guided by the following six principles:

1. Data will be processed lawfully, fairly and in a transparent manner in relation to individuals.
2. Data will be collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes shall not be considered to be incompatible with the initial purposes.
3. Data will be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
4. Data will be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay.
5. Data will be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
6. Data will be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

How to Use This Toolkit
Use this toolkit to understand the GDPR's requirements, assess your own compliance and document your efforts. This toolkit contains sample policies that require customisation. Although the policies are not GDPR-specific, such as the BYOD and Acceptable Use Policy, customising these policies and ensuring all employees heed them will form an integral part of demonstrating your commitment to accountability, data security and robust documentation. Customised, internal policies governing how employees should handle data will also help prove that your organisation values data security and that 'data protection by design and default' is baked into its very fabric—a key obligation under the GDPR.

Regulatory
Update

EU General Data Protection Regulation

Provided by RS Risk Solutions Ltd

Quick Facts

- The data protection rules became effective on 25 May 2018.
- The new rules replaced the 1995 and 2008 standards and directives.
- Fines for non-compliance can be up to €20 million or 4 per cent of annual global turnover.

The GDPR enables individuals to better control their personal data, regardless of where this data is sent, stored or processed.

Data Protection Reform

The EU's new data protection reform was published on 4 May 2016. The new rules became applicable on 25 May 2018. Because of how the rules are set up, member states are not required to adopt local laws to incorporate the new data protection requirements into domestic legislation.

The EU enacted these rules to create uniform data protection rules for all member states. In its view, a unified set of rules and standards would allow EU citizens more control over their personal information. Organisations that trade in the EU, whether based there or not, must comply with these rules in regards to processing the data of their EU customers.

These rules updated and replaced the 1995 Data Protection Directive and the 2008 Framework Decision for the police and criminal justice sector.

Data protection reform takes place through two major instruments:

- The General Data Protection Regulation (GDPR); and
- The Data Protection Directive.

Enforcement

A company that fails to comply with the rules may be subject to a fine of up to €20 million, or 4 per cent of the company's global annual turnover (whichever is greater).

The GDPR

The GDPR enables individuals to better control their personal data, regardless of where this data is sent, stored or processed. The GDPR has four provisions which provide:

- **Individuals with more access to their own data**—individuals will have more information on how their data is processed (this information must be provided in a clear and transparent way);
- **A right to data portability**—by making it easier for individuals to transmit their personal data between service providers;
- **A 'right to be forgotten'**—individuals have a right to have their personal data erased if there is no legitimate ground for retaining the data; and
- **Individuals with the right to know when their information has been hacked**—by creating an obligation for those who gather, store or process personal data to notify their respective national supervisory authority of any data breaches that put them at risk (notifications should be given as soon as possible so that affected individuals can take appropriate measures).

The GDPR eliminated the obligation for businesses to notify other national data protection authorities about the data they are processing, which cost businesses about €130 million per year, according to the European Commission.

Consent and Specific Purpose
The 'right to be forgotten' is tied to two concepts— **specific purpose** and **consent**.

The GDPR assumes that when an individual consents to the processing of his or her personal data, he or she does so because that data is intended for the individual's benefit or some other specific purpose.

For this reason, individuals have a right to request that their personal data be erased when processing this data is no longer required in order to meet the specific purpose for which consent was given.

However, an individual's right to be forgotten is not absolute. Data does not need to be erased if a legitimate purpose remains. Legitimate purposes include freedom of expression and scientific research.

Finally, the GDPR also recognises that a certain level of maturity and understanding is required in order to provide consent for a specific purpose. For this reason, one GDPR rule indicates that consent, for the processing of a child's personal information, must be given by whoever holds that child's parental responsibility, until the child is deemed sufficiently old enough to give consent. The GDPR allows member states to set their own age limit standard between 13 and 16 years of age.

Data Protection Directive
The Data Protection Directive applies to the police and criminal justice sectors. The directive was adopted to protect the personal data of victims, witnesses and suspects in a criminal investigation or law enforcement action.

The directive also facilitates the sharing of information and cross-border cooperation to combat crime and terrorism.

Impact on Businesses
The reforms create a more efficient business environment by cutting red tape and reducing the costs many businesses must endure if they process personal data across borders. Businesses may be able to capitalise on simpler, clearer and more unified standards as they restore or maintain consumer trust.

The reforms also make new data protection standards extraterritorial by requiring all businesses to comply while they do business in an EU member state. This ensures that all players within the EU are bound by the same rules, regardless of where they are established.

In addition, the rules streamline data safety by creating one central, single supervisory authority in each member state. It also promotes a risk-based approach to compliance requirements, recognising that businesses should have different obligations and operate under standards that more accurately represent the particular risk associated with their data processing.

Finally, the new rules call for data processors to implement data protection safeguards from the early stages of product and service development to ensure that data protection becomes the norm—by design and by default. This includes appointing a data protection officer (DPO) responsible for data protection compliance. Organisations must appoint a DPO if they are a public authority, they carry out large-scale systematic monitoring of individuals, or if they carry out large-scale processing of special categories of data or data relating to criminal convictions and offences.

Impact on Small and Medium Enterprises
The new rules also level the playing field for SMEs by requiring them to:

- Appoint DPOs only when the SMEs' core activities require regular and systematic monitoring, or if they process special categories of personal data (for example, data that reveals racial origin or religious belief);

The GDPR established a single, pan-European law for data protection, meaning that companies only have to deal with one law, not 28. The new rules bring benefits of an estimated €2.3 billion per year, according to the European Commission.

- Keep processing records only if processing is not occasional or is likely to put rights and freedoms at risk; and
- Report data breaches to individuals only if the breaches place their rights and freedoms at high risk.

In situations where SMEs must appoint DPOs, the new rules do not require that officers be full-time employees. The use of *ad hoc* and consultants is sufficient to satisfy this requirement.

Impact on Employers

Employers process a large amount of personal data from their employees. Often, processing employee information is necessary to comply with employment law and to provide adequate benefits.

For this reason, employers should evaluate how the GDPR affects their personal data processing practices, policies and procedures. In particular, employers should consider whether they have obtained consent for a specific purpose and delineate when and how this consent may lapse.

Complying with the GDPR

The Information Commissioner's Office (ICO) has created a checklist of things businesses can do to ensure GDPR compliance:

1. **Awareness:** Ensure that all decision makers and key people in your organisation are aware of the GDPR—they need to appreciate its impact.
2. **Information You Hold:** Document what personal data you hold, where it came from and whom you share it with. Also, organise an information audit.
3. **Communication of Privacy Information:** Review your current privacy notices and put a plan in place for making any necessary GDPR changes.
4. **Individuals' Rights:** Check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.
5. **Subject Access Requests:** Update your procedures and plan how you will handle requests within the new timescales and provide any extra information.
6. **Legal Basis for Processing Personal Data:** Look at the various types of data processing you carry out, identify your legal basis for doing so and document it.
7. **Consent:** Review how you are seeking, obtaining and recording consent and whether you need to make any changes.
8. **Children:** Think about putting systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity.
9. **Data Breaches:** Ensure you have the right procedures in place to detect, report and investigate data breaches.
10. **Data Protection by Design and Data Protection Impact Assessments:** Familiarise yourself with the guidance the ICO has produced on Privacy Impact Assessments, and work out how and when to implement them.
11. **Data Protection Officers:** Designate a DPO, if required, or someone to be responsible for data protection compliance, and assess where this role will sit within your organisation's structure and governance arrangements.
12. **International:** If your organisation operates internationally, you should determine which data protection supervisory authority you fall under.

For a more detailed overview of your responsibilities under the GDPR, consult the ICO's guide for organisations located here. And for more information on protecting your business and ensuring compliance, contact the insurance professionals at RS Risk Solutions Ltd today.

GDPR Compliance Timeline

Raise Awareness, Gather Information (2016-2017)

- Inform board members of the impact that the GDPR will have on your business.
- Conduct an information audit and record how you collect, store and use personal data.
- Verify that your legal grounds for processing personal data are legitimate.
- Review IT systems and procedures as well as staffing requirements for data protection compliance.

Plan and Prioritise Compliance Efforts (January to May 2017)

- Recruit and appoint a data protection officer (not necessary for all organisations).
- Develop a comprehensive privacy compliance programme that holds you accountable.
- Prioritise personal data compliance activities throughout your organisation.
- Conduct a data protection impact assessment.
- Identify your riskiest data processing activities and strengthen your protection.
- Establish procedures to identify data breaches as well as to inform the ICO and affected individuals.

Implement Changes (June 2017 to January 2018)

- Integrate privacy data by design and default into each of your processes.
- Review and update privacy policies and notices.
- Review and audit legacy contracts.

Embed Change, Train and Retrain (January to May 2018)

- Provide GDPR training for your entire organisation that includes:
    - How to be compliant
    - How to recognise and identify a data breach
    - How to report a data breach
- Consider earning applicable codes and certifications, which can help with compliance on security and data transfers.

Monitor, Review and Revise (Ongoing)

- Monitor your GDPR compliance efforts.
- Reassess whether your efforts are still effective. If not, make changes.
- Provide annual GDPR training for your organisation.

12 Steps to Take to Prepare for the GDPR

Step 1: Awareness

Make sure that decision makers and key people in your organisation are aware that the law is changing. They need to appreciate the GDPR's impact.

Step 2: Information You Hold

Document what personal data you hold, where it came from and with whom you share it. You may need to organise an internal audit.

Step 3: Communicating Privacy Information

Review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

Step 4: Individuals' Rights

Check your procedures to ensure they cover individuals' rights, including how you would delete personal data or provide data electronically in a commonly used format.

Step 5: Subject Access Requests

Update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

Step 6: Lawful Basis for Processing Personal Data

Identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

Step 7: Consent

Review how you seek, record and manage consent, and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

Step 8: Children

Think about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

Step 9: Data Breaches

Make sure you have the right procedures in place to detect, report and investigate a personal data breach.

Step 10: Data Protection by Design and Impact Assessments

Familiarise yourself with the ICO's code of practice on privacy impact assessments along with Article 29 Working Party, then implement them.

Step 11: Data Protection Officers

Designate someone to take responsibility for data protection compliance or consider whether you are required to formally designate a data protection officer.

Step 12: International

If your organisation operates in several EU member states, including cross-border processing, you should determine your lead data protection supervisory authority.

International Data Transfers Under the GDPR

The GDPR imposes restrictions on the transfer of personal data outside the EU to other countries or international organisations.

Transfers may be made when the EU Commission has decided that a third country (which is a country outside of the EU), a territory or one or more specific sectors in the third country, or an international organisation ensures an adequate level of protection.

In the absence of such a decision, you may complete a transfer of personal data outside the EU if the recipient provides at least one of the following safeguards:

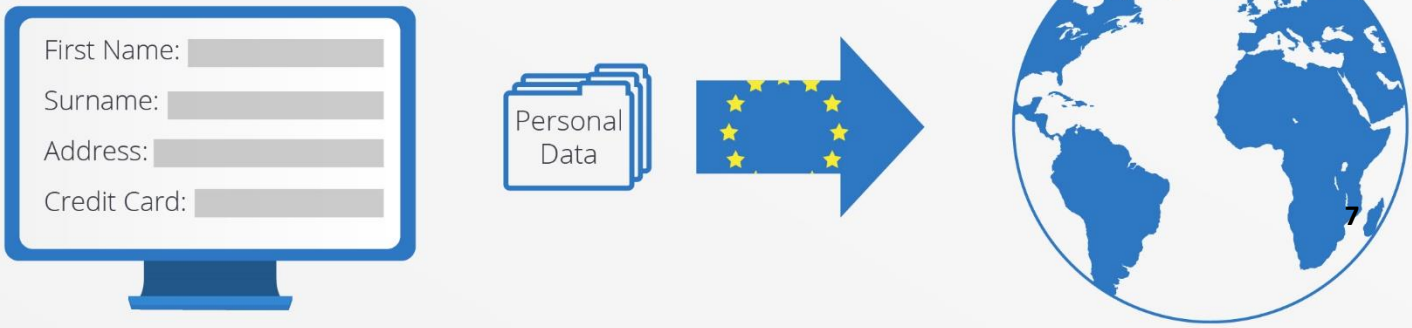
- ☐ A legally binding agreement between public authorities or bodies
- ☐ Binding corporate rules
- ☐ Standard data protection clauses adopted by the EU Commission
- ☐ Standard data protection clauses adopted by a supervisory authority and approved by the EU Commission
- ☐ Compliance with an approved code of conduct approved by a supervisory authority
- ☐ Certification provided by the GDPR
- ☐ Contractual clauses agreed and authorised by the supervisory authority
- ☐ Provisions inserted into administrative agreements authorised by the supervisory authority

In the absence of an EU Commission decision or the appropriate safeguards, you may still undertake the international transfer if it meets at least one of the following conditions:

- ☐ It will be made with the individual's informed consent.
- ☐ It is necessary for the performance of a contract between the individual and the organisation.
- ☐ It is necessary for the performance of a contract made in the interests of the individual.
- ☐ It is necessary for important public interests reasons.
- ☐ It is necessary for the establishment, exercise or defence of legal claims.
- ☐ It is necessary to protect the vital interests of the individual or other people in the event that they are physically or legally unable to provide consent.
- ☐ It is made from a register.

Even when there is not an EU Commission, there are no adequate safeguards and none of the exemptions apply, you may transfer the data as long as it meets the following conditions:

- ☐ The data transfer is not being made by a public authority in the exercise of its public powers.
- ☐ The data transfer is not repetitive.
- ☐ The data transfer involves data related to only a limited number of individuals.
- ☐ The data transfer is necessary for the purposes of the compelling legitimate interests of the organisation.
- ☐ The data transfer is made subject to suitable safeguards put in place by the organisation .



Key Facts About the **GDPR**

WHAT RIGHTS DOES THE GDPR GIVE INDIVIDUALS?

- **Right to be informed:** Organisations must be transparent about how they use personal data
- **Right of access:** Individuals have the right to access their personal data
- **Right to rectification:** Individuals have the right to have their personal data rectified (for example, if it's inaccurate or incomplete)
- **Right to erasure:** Individuals have the 'right to be forgotten'—meaning, they have the right to have their data deleted
- **Right to restrict processing:** Individuals have the right to block or suppress processing of personal data
- **Right to data portability:** Individuals have the right to obtain and reuse their personal data for their own purposes across different services
- **Right to object:** Individuals have the right to object to processing of their personal data
- **Rights in relation to automated decision making and profiling**

HOW MUCH CAN I GET FINED?

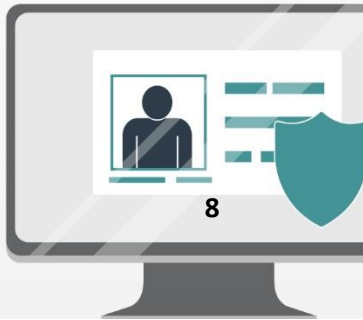
- **€10 million (roughly £8 million) or 2% of your annual turnover—whichever is higher**—for not keeping proper records, violating data breach notification requirements, failing to appoint a data protection officer when necessary and more
- **€20 million (roughly £16 million) or 4% of your annual turnover—whichever is higher**—for violating the basic principles for processing, ignoring data subjects' rights, incorrectly transferring personal data and more

WHAT QUALIFIES AS PERSONAL DATA?

Any information that can directly or indirectly identify a person, such as:

- Name, identification number, location data or an online identifier
- Factors specific to a person's physical, physiological, genetic, mental, economic, cultural or social identity

If you're unsure whether something is personal data, the best practice is to treat it as such.



RISK INSIGHTS

Marketing Under the GDPR

Since its introduction, the General Data Protection Regulation (GDPR) has been poised to radically change the way that organisations handle their digital business operations. The GDPR expands the rights of individuals and their data, and places greater obligations on organisations that process personal data.

In order to comply, there are a number of revisions and adjustments that your organisation must make to your digital business practices, including your marketing and advertising efforts. If your organisation does not follow the revised regulations, you could receive significant fines and face prosecutions by the Information Commissioner's Office (ICO). One of the most effective methods to market under the GDPR is to highlight the content that your organisation can provide as a way to gain individuals' consent.

To ensure that your organisation effectively markets under the GDPR, it is essential that you understand consent along with how the new regulations impact your digital marketing and advertising efforts.

Overview of PECR, the GDPR's Marketing Guidelines

The GDPR's main focus is the protection of personal data and included under that umbrella is the Privacy and Electronic Communications Regulations (PECR), which specifically deals with electronic communications.

While PECR has existed since 2003, it is currently undergoing a major overhaul to adequately supplement the GDPR and update electronic marketing rules. The proposed revisions to PECR include simplifying cookies, banning unsolicited electronic communications if users haven't given their consent and incorporating the GDPR's two-tiered fine structure.

PECR's biggest proposed change is making all forms of electronic marketing reliant on opt-in consent. Similar to the GDPR, this means that pre-ticked boxes will no longer be acceptable, even with business-to-business communications. Now, your organisation must identify and provide a lawful basis to process personal data, which is any information that can be used to identify an individual. Put simply, joe.public@anybusiness.com would classify as personal data that requires Joe's consent before you can market to him through email, even though it's a business address.

> The GDPR impacts how your organisation is able to conduct its digital marketing and advertising practices. If you don't make the necessary adjustments, you could receive a €20 million fine.

However, even though EU lawmakers intend for these proposed changes to PECR to take effect on 25 May, the same day as the GDPR, there's significant doubt as to whether they will make that deadline. Regardless, as PECR is a part of the GDPR, your organisation should follow the revised marketing guidelines to avoid potential fines.

Potential Consequences of Non-compliance

Under the GDPR, the ICO has the authority to mete out more substantial fines to organisations that don't comply with the new regulations. If you are found to

be non-compliant, you could receive one of the GDPR's two-tiered fines:

- A fine of up to €10 million (roughly £8 million) or 2 per cent of your annual turnover—whichever is higher—can be given for the following causes:
    - Not properly filing and organising personal data records
    - Not notifying the supervising authority (such as the ICO) and affected individuals about a breach
    - Not conducting the necessary preliminary impact assessments
- A fine of up to €20 million (roughly £16 million) or 4 per cent of your annual turnover—whichever is higher—can be given for the following causes:
    - Violating the basic principles related to data security
    - Violating consumer consent

Even though your organisation could receive either fine, you would most likely receive the more substantial fine for any violations in your digital marketing and advertisement practices.

Real World Examples of Attempted GDPR Compliance

Even with all the available guidance on GDPR compliance, some organisations may find implementing and following the necessary changes difficult. Despite their best intentions and efforts, organisations that strive to comply with the GDPR while disregarding other regulations, such as PECR, will be held liable by the ICO. The ICO has cautioned that, 'Businesses must understand they can't break one law to get ready for another'. To ensure that your organisation doesn't make the same mistakes, here are several examples of organisations that incorrectly followed the GDPR.

Flybe

Flybe, a British airline, was fined £70,000 after it sent more than 3.3 million marketing emails to individuals that had opted out of receiving them. The emails were intended to amend out-of-date personal information as well as to update their marketing preferences in anticipation of the GDPR. To encourage individuals to provide the requested information, the airline offered them the chance to be entered into a prize drawing. However, since the airline deliberately sent emails to individuals who had specifically opted out of Flybe marketing emails, the ICO found the airline to be in violation of PECR.

Honda

Honda Motor Europe Ltd was fined £13,000 after it sent nearly 300,000 unsolicited emails to individuals. The emails were intended to clarify customers' choices for receiving marketing spam and help the company comply with the GDPR. However, as the company viewed the emails as a part of customer service rather than marketing, Honda did not attempt to obtain its customers' consent. During its investigation of the incident, the ICO determined that the emails were used as a marketing tool and, as such, violated PECR.

Morrisons

UK supermarket chain Morrisons was fined £10,500 after it sent out 230,000 emails to members from its database, asking them to update their account preferences. However, of those that received the email, 131,000 had previously opted out and unsubscribed. As Morrisons did not have the express consent of its customers, it was in violation of PECR.

Obtaining Consent is Key

One of the most significant changes introduced by the GDPR is strengthening the standards of obtaining consent to process personal data. Failure to obtain proper consent puts your organisation at risk for significant fines.

In order for your organisation to remain compliant with the GDPR in your electronic marketing and advertising efforts, your process for obtaining consent must meet the following standards:

- **Unbundled**—Consent requests must be separate from other terms and conditions, and should not be a precondition of signing up for a service.
- **Active opt-in—**Your organisation cannot use pre-ticked opt-in boxes.
- **Granular**—Provide options to individuals to consent to different types of processing.
- **Named**—Provide the name of your organisation and any third parties that will be relying on the individuals' consent.
- **Documented**—Keep records that demonstrate what the individuals have consented to, what they were told, and when and how they have consented.
- **Easy to withdraw**—Inform the individuals that they have the right to withdraw their consent at any time and explain how they can do that.
- **No imbalance in the relationship**—Consent will not be considered freely given if there is an imbalance in the relationship between the individuals and your organisation.

Advice for Marketing Under the GDPR

There are three main areas that your organisation may want to consider when marketing under the GDPR:

- **Data permission**—This refers to how your organisation manages your email opt-ins.
- **Data access**—This refers to the individual's right to access their personal data and remove consent for its use.
- **Data focus**—This refers to your organisation having to legally justify the lawful basis for the processing of all the personal data you collect.

Fortunately, marketing under the GDPR can be an easy endeavour by following these best practices:

- Review how your organisation collects, processes, stores and removes personal data.
- Identify which of the six lawful bases applies to your personal data processing, and document your rationale for collecting personal data.
- Ensure that your process for obtaining consent meets the necessary standards. In addition, you may want to implement a double opt-in practice, which asks individuals to take an additional step to confirm their email address and provide consent.
- Audit your mailing list to ensure that the collected customer data meets GDPR requirements. If you identify any individuals that don't have a record of their opt-in, you must delete them from your database.
- Educate your sales team about social media selling techniques, such as connecting with prospects on social media and sharing relevant content with them. The reason for this is that social media sites have privacy notices built into them.
- Create a content marketing strategy to provide individuals with relevant, useful content that incentivises them to give their consent. It could be a brief about important legislation, a hazard that impacts their sector, or health and safety guidance. Just remember not to make the content contingent on the individual giving their consent—this could mean consent was not freely given and thus make it invalid.

Remember: Content Incentivises Consent

The GDPR has considerably adjusted the guidelines for how organisations can manage their digital marketing and advertising efforts. Obtaining consent is now central to establishing the necessary lines of communication with individuals, yet making that connection is not always easy. However, by highlighting the quality and benefits of the content your organisation can provide, individuals may be more likely to give consent.

For additional guidance on how your organisation can effectively operate under the GDPR, contact the professionals at RS Risk Solutions Ltd today.

POLICY

Bring Your Own Device (BYOD) and Acceptable Use

Location: [INSERT LOCATION]
Effective Date: [INSERT DATE]
Revision Number: [INSERT #]

About This Policy

Information security policies are the principles that direct managerial decision making and facilitate secure business operations. A concise set of security policies enables the IT team to manage the security of information assets and maintain accountability. These policies provide the security framework upon which all subsequent security efforts will be based. They define the appropriate and authorised behaviour for personnel approved to use information assets, such as laptops, tablets and smartphones.

Applicability

The BYOD and Acceptable Use Policy applies to all employees, interns, contractors, suppliers and anyone using assets. Policies are the organisational mechanism used to manage the confidentiality, integrity and availability issues associated with information assets. Information assets are defined as any information system (hardware or software), data, networks, and components owned or leased by or its designated representatives.

BYOD POLICY

This policy provides guidelines for using personally owned devices and related software for corporate use.

Applicability

The BYOD policy applies to all employees, contractors, suppliers and any other person using or accessing information or information systems. Exceptions to this policy must be approved by appropriate management or a designated representative.

Furthermore, based on the amount of personally identifiable information employees work with, management reserves the right to determine which employees can use personally owned devices and which cannot.

General Policy

recognises that personally owned equipment can play a valuable role in convenience, efficiency and productivity of its employees. Nonetheless, the use of these devices must be monitored closely.

The following is a list of personally owned devices permitted by for corporate use:

- Desktop computers
- Laptop computers
- Tablets
- Personal digital assistants (PDAs)
- Smart phones
- Portable music players

Reimbursement

may provide reimbursement for the purchase of personally owned devices up to £_____ to eligible employees. However, is not responsible for any additional costs associated with learning, administering or installing these devices.

Registering Devices

All personally owned devices must be registered with ’s IT department.

End-User Support

As a general rule, users of personally owned devices will not use or request corporate IT resources in the use, network connectivity or installation of their equipment or software. Users are responsible for learning, administering, installing and setting up their personally owned devices.

IT will support personally owned devices as follows:

- The user will be required to allow IT to load security software on each device.

- The user will be required to allow IT to install remote wiping software on each device.
- Upon request, the IT team will install the necessary synchronisation software to the user's desktop or notebook computer.

Device Security

The user should follow good security practices including:

- Password protect all personally owned devices
- Do not leave personally owned devices unattended

Release of Liability and Disclaimer to Users

hereby acknowledges that the use of personally owned devices in connection with business carries specific risks for which you, as the end user, assume full liability. In the case of litigation, may take and confiscate a user's personally owned device at any time.

ACCEPTABLE USE POLICY

This policy provides rules for the acceptable use of personally owned devices on the corporate network.

Applicability

The Acceptable Use Policy applies to all employees, contractors, suppliers and any other person using or accessing information or information systems. Exceptions to this policy must be approved by the CIO or a designated representative.

General Policy

Users that wish to access the network using their personally owned computer may do so using only -authorised software and only with the approval of the user's supervisor and the IT department. Users must follow the same rules when accessing the network from both corporate-issued equipment and personally owned devices. When connected to the network, the user will NOT:

- Use the service as part of violating the law
- Attempt to break the security of any computer network or user
- Attempt to send junk email or spam to anyone
- Attempt to send a massive amount of email to a specific person or system in order to flood their servers

Authorisation of Devices

IT reserves the right to determine the level of network access for each personally owned device. The user could be granted full, partial or guest access. IT will install a digital certificate on each personally owned device, which will authenticate the user.

Third-Party Applications on Devices

IT reserves the right to block or limit the use of certain third-party applications, such as those that probe the network or share files illegally, that may harm the corporate network. As the number of approved applications continually evolves, the user must check with the IT department for the current list of approved third-party applications and get IT approval before downloading it on the device.

Remote Wiping

While does not own the device, they do own all company data. Therefore, reserves the right to remotely wipe the user's personally owned device at any time. Not only will company data get wiped, but the user's personal data could be lost as well. The user must understand and accept this risk. Furthermore, the user must agree to a full wipe of the personally owned device if they leave . This may result in the loss of both company and personal data on the device

Reporting Security Concerns

The user agrees to report the following immediately:

- If the device is lost or stolen
- If the device has been attacked with malware, a virus or any other suspicious attack
- Any other security concern with regards to company data

Release of Liability and Disclaimer to Users

hereby acknowledges that the use of a personally owned device on the network carries specific risks for which you, as the end user, assume full liability.

Bring Your Own Device (BYOD) and Acceptable Use Policy

Security of information, and the tools that create, store and distribute that information are vital to the long-term health of our organisation. It is for this reason we have established our BYOD and Acceptable Use Policy.

All employees are expected to understand and actively participate in this programme. encourages its employees to take a proactive approach in identifying potential problems or violations by promptly reporting them to their supervisor.

Prior to using personal devices for company purposes, each employee is expected to have read the entire BYOD and Acceptable Use Policy.

If you have any uncertainty regarding the content of these policies, you are required to consult your supervisor. This should be done prior to signing and agreeing to the BYOD and Acceptable Use Policy.

I have read and understand 's BYOD and Acceptable Use Policy, and I understand the requirements and expectations of me as an employee.

Employee Signature: _____ Date: _____

POLICY

General Email / Internet Security and Use

Location: [INSERT LOCATION]
Effective Date: [INSERT DATE]
Revision Number: [INSERT #]

GENERAL SECURITY POLICY

The General Email/Internet Security and Use Policy forms the foundation of the corporate Information Security Programme. Information security policies are the principles that direct managerial decision making and facilitate secure business operations. A concise set of security policies enables the IT team to manage the security of information assets and maintain accountability. These policies provide the security framework upon which all subsequent security efforts will be based. They define the appropriate and authorised behaviour for personnel approved to use information assets.

Applicability

The General Email/Internet Security and Use Policy applies to all employees, interns, contractors, suppliers and anyone using assets. Policies are the organisational mechanism used to manage the confidentiality, integrity and availability issues associated with information assets. Information assets are defined as any information system (hardware or software), data, networks and components owned or leased by or its designated representatives.

General Policies

All employees, contractors, suppliers and any other person using or accessing information or information systems must adhere to the following policies.

- All information systems within are the property of and will be used in compliance with policy statements.
- Any personal information placed on information system resources becomes the property of .
- Any attempt to circumvent security policy statements and procedures (ie, disconnecting or tunnelling a protocol through a firewall) is strictly prohibited.
- Unauthorised use, destruction, modification and/or distribution of information or information systems is prohibited.
- All users will acknowledge understanding and acceptance by signing the appropriate policy statements prior to use of information assets and information systems.
- At a minimum, all users will be responsible for understanding and complying with the following policy statements:
    - General Security Policy
    - System Security Policy
    - Desktop Service Security Policy
    - Internet Acceptable Use Policy
    - Personal Equipment Policy
    - Virus, Hostile and Malicious Code Policy
- All users will report any irregularities found in information or information systems to the IT team immediately upon detection.
- information systems and information will be subject to monitoring at all times. Use of information systems constitutes acceptance of this monitoring policy.
- Use of any information system or dissemination of information in a manner bringing disrepute, damage or ill-will against is not authorised.
- Release of information will be in accordance with Policy Statements

- Users will not attach their own computer, test equipment or personal software (including software applications) to computers or networks without prior approval of the IT team or its designated representative.
- If a user fails to comply with this policy, he or she will face disciplinary proceedings, up to and including dismissal.

SYSTEM SECURITY POLICY

's System Security Policy addresses access control, use of hardware, operating systems, software, servers and backup requirements for all systems maintained and operated by .

Applicability

The System Security Policy applies to all employees, contractors, suppliers and any other person using or accessing information or information systems. Exceptions to this policy must be approved by the CIO or a designated representative.

Password System Security

In today's information age, poorly selected, reusable passwords represent the most vulnerable aspects of information security. has adopted this policy to ensure that the private information of our clients and our proprietary corporate data are kept secure at all times. -authorised users must comply with creation, usage and storage policies to minimise risk to corporate information assets.

- Passwords will conform to the following criteria:
    - Passwords will be a minimum of [insert number] characters
    - Passwords must also contain [edit as needed, for example: at least one uppercase letter, one lowercase letter and one number].
- The sharing of passwords is prohibited.
- Any suspicious queries regarding passwords will be reported to the IT team.
- Passwords will be protected as proprietary information. Writing them down or storing them unencrypted on the information system is prohibited.
- Users will be forced to change passwords every [insert number] days and may reuse passwords only after [insert number] different passwords have been used.
- Accounts will be locked out after [insert number] failed password attempts in a [insert number]-minute time period. Accounts can be reset by contacting the IT team or by waiting [insert number] minutes for the account to reset automatically.
- Users will be forced to unlock their computers using their network password after [insert number] minutes of inactivity on their desktops.
- All system passwords will be changed within [insert number] hours after a possible compromise.
- When users leave the organisation, their accounts will be deleted.
- If the user leaving the organisation was a privileged user or a network administrator, all system passwords will be changed.

DESKTOP SERVICES SECURITY POLICY

The Desktop Services Security Policy addresses the authorised and legitimate use of hardware, operating systems, software, LAN, file servers and all other peripherals used to access any information system.

- No software of any kind will be installed onto a laptop or desktop computer without the approval of the IT team.
- Only system administrators will have the ability to install software.
- Unauthorised copying or distributing of copyrighted software is a violation of UK Copyright Law and will not be permitted.
- Personal software (including software applications) will not be installed on any machine.
- Users will not allow non-employees to use any machine or device without authorisation of the IT team.

- The following items are corporate policy for security monitoring:
    - All systems and network activities will be subject to monitoring. Use of systems and networks constitutes consent to this monitoring.
    - Disabling or interfering with virus protection software is prohibited.
    - Disabling or interfering with logging, auditing or monitoring software is prohibited.
    - All desktop services will be subject to inventory and inspection.
    - Security irregularities, incidents, emergencies and disasters related to information or system will be reported to the IT team immediately.
- The following items are corporate policy for system usage:
    - Sabotage, destruction, misuse or unauthorised repairs are prohibited on information systems.
- All repairs will be authorised and performed by the IT team.
    - Desktop resources will not be used to compromise, harm, destroy or modify any other service or resource on the information system.
    - All data on information systems at is classified as company proprietary information.
    - Users will secure all printed material and other electronic media associated with their use of information and information systems.
    - Storage, development or the unauthorised use of tools that compromise security (such as password crackers or network sniffers) are prohibited.

INTERNET ACCEPTABLE USE POLICY

Internet access is provided to employees to conduct business. While these resources are to be used primarily for business, the company realises that employees may occasionally use them for personal matters and therefore provides access to non-offensive personal sites during non-business hours.

- Non-business Internet activity will be restricted to non-business hours. actively blocks non-business sites during working hours. Working hours are defined as [insert working hours, for example: Monday – Friday from 7:00–12:00 and from 12:45–17:00 hours].
- The definition of non-business sites is the sole discretion of the IT team. This definition may change without notice as the Internet continues to evolve.
- Internet activity will be monitored for misuse.
- Internet activities that can be attributed to a domain address (such as posting to newsgroups, use of chat facilities and participation in email lists) must not bring disrepute to or associate with controversial issues (ie, sexually explicit materials).
- Internet use must not have a negative effect on operations.
- Users will not make unauthorised purchases or business commitments through the Internet.
- Internet services will not be used for personal gain.
- Internet users will make full attribution of sources for materials collected from the Internet. Plagiarism or violation of copyright is prohibited.
- Release of proprietary information to the Internet (ie, posting information to a newsgroup) is prohibited.
- All Internet users will immediately notify the IT team of any suspicious activity.
- All remote access to the internal network through the Internet will be encrypted and authenticated in a manner authorised by the IT team.
- Accessing personal social networking accounts (including but not limited to Facebook®, Twitter®, Google+®, MySpace®, LinkedIn®, Foursquare® and TUMBLR®) or using email for personal social networking purposes is prohibited during working hours. The use of social networking sites for specific business purposes must be pre-approved or assigned by a manager/supervisor.

EMAIL SECURITY POLICY

The Email Security Policy specifies mechanisms for the protection of information sent or retrieved through email. In addition, the policy guides representatives of in the acceptable use of email. For this policy, email is described as any computer-based messaging including notes, memos, letters and data files that may be sent as attachments.

Applicability

The Email Security Policy applies to all employees, contractors, suppliers and any other person using or accessing information or information systems. Exceptions to this policy must be approved by the CIO or his/her designated representative.

Policy

Authorised users are required to adhere to the following policies. Violators of any policy are subject to disciplinary actions, up to and including termination.

The following items are the corporate policy statements for Access Controls:

All email on the information systems, including personal email, is the property of . As such, all email can and will be periodically monitored for compliance with this policy.

Individual email accounts are intended to be used only by the person to whom they are assigned. Special arrangements can be made to share information between team members, such as between a producer and an account representative. In all other cases, no user is authorised to open or read the e-mail of another without the express consent of senior management.

Email is provided to the users of primarily to enhance their ability to conduct business.

Email will be stored on the system up to a maximum of [insert number] MB per mailbox. Mailbox is defined as the combined total of deleted items, inbox, sent items and any user-created email folders. Users will receive a warning message stating that they need to clear out space when their mailbox size reaches [insert number] MB. However, once the mailbox storage space exceeds [insert number] MB, users will not be able to send new messages until the mailbox size falls below the [insert number] MB limit. In all cases, however, users will continue to receive incoming messages.

The maximum size of any individual incoming email message will be [insert number] MB.

Terminated employees will have all email access immediately blocked.

Users who leave the company will have all new e-mails automatically forwarded to their supervisor, or their designated representative, for [insert number] days.

The former employee's supervisor is responsible for disseminating stored emails to the appropriate party. Thirty days after the date of termination, the former employee's mailbox will be permanently removed from the system.

The following items are the corporate policy statements for Content:

- Use of profane, inappropriate, pornographic, slanderous or misleading content in email is prohibited.
- Use of email to spam (ie, global send) is prohibited. This includes the forwarding of chain letters.
- Use of email to communicate sexual or other harassment is prohibited. Users may not include any words or phrases that may be construed as derogatory based on race, colour, sex, age, disability, national origin or any other category.
- Use of email to send unprofessional or derogatory messages is prohibited.
- Forging of email content (ie, identification, addresses) is prohibited.
- All outgoing email will automatically include the following statement: [insert company email confidentiality statement, for example: "This email is intended solely for the person or entity to which it is addressed and may contain confidential and/or privileged information. Any review, dissemination, copying, printing or other use of this email by persons or entities other than the addressee is prohibited. If you have received this email in error, please contact the sender immediately, and delete the material from your computer."]

The following items are the corporate policy statements for Usage:

Any email activity that is in violation of policy statements or that constitutes suspicious or threatening internal or external activity will be reported.

When sending email, users should verify all recipients to whom they are sending the message(s).

Be aware that deleting an email message does not necessarily mean it has been deleted from the system.

PERSONAL EQUIPMENT POLICY

This policy provides guidelines for using corporate IT support resources for personally owned equipment and related software including, but not limited to: notebook computers, desktop computers, personal digital assistants (PDAs), smartphones and mobile phones.

Applicability

The Personal Equipment Policy applies to all employees, contractors, suppliers and any other person using or accessing information or information systems. Exceptions to this policy must be approved by the CIO or his/her designated representative.

General Policy

recognises that personally owned equipment can play a valuable role in convenience, efficiency and productivity of its employees. Nonetheless, the use of corporate resources, human or otherwise, for personal gain must be monitored closely.

As a general rule, employees of will not use or request corporate IT resources in the use, network connectivity or installation of their personally owned equipment or software.

Personally owned notebooks and desktop computers will not be granted direct physical access to the network. Employees that wish to access the network from a remote location using their personally owned computer may do so using only -authorised software and only with the approval of the employee's supervisor or manager.

PDAs and smart phones, which include devices using BlackBerry®, iPhone®, Windows Mobile®, Android®, Linux® and Palm® technologies, will be supported according the following rules:

- Employees are responsible for learning, administering, installing and setting up their own PDAs or smartphones.
- Corporate IT resources should not be used for assistance in the basic operation of these devices.
- Upon request, the IT team will install the necessary synchronisation software to the employee's desktop or notebook computer.

VIRUS, HOSTILE AND MALICIOUS CODE SECURITY POLICY

The intent of this policy is to better protect assets against attack from destructive or malicious programmes.

- Any public domain, freeware or shareware software will be evaluated by the IT team prior to installation on any company resource.
- No unauthorised software will be downloaded and installed on end user machines without express approval from the IT team.
- System users will not execute programmes of unknown origin, as they may contain malicious logic.
- Only licensed and approved software will be used on any company computing resource.
- All licensed software will be write-protected and stored by the IT team.
- users will scan all files introduced into its environment for virus, hostile and malicious code before use.
- The IT team will ensure that obtains and deploys the latest in virus protection and detection tools.
- All information systems media, including disks, CDs and Universal Serial Bus (USB) drives, introduced to the environment will be scanned for virus, hostile and malicious code.
- All emails will be scanned for virus, hostile and malicious code.
- All Internet file transfers will be scanned for virus, hostile and malicious code.
- The unauthorised development, transfer or execution for virus, hostile and malicious code is strictly prohibited.
- All users will report any suspicious occurrences to his/her supervisor or the IT team immediately.
- All company systems will be protected by a standard virus protection system.
- Virus engines and data files will be updated on at least a monthly basis.
- Viruses that are detected on a user's workstation will be reported to the IT team immediately for action and resolution.
- Anomalous behaviours of any software programme will be reported to the IT team immediately.

General Email/Internet Security and Use Policy

Security of information, and the tools that create, store and distribute that information are vital to the long-term health of our organisation. It is for this reason we have established our General Email/Internet Security and use Policy.

All employees are expected to understand and actively participate in this programme. encourages its employees to take a proactive approach in identifying potential problems or violations by promptly reporting them to their supervisor.

Prior to using equipment, each employee is expected to have read the entire General Email/Internet Security and Use Policy, which includes:

- General Security Policy
- System Security Policy
- Desktop Service Security Policy
- Internet Acceptable Use Policy
- Personal Equipment Policy
- Virus, Hostile and Malicious Code Policy

If you have any uncertainty regarding the content of these policies, you are required to consult your supervisor. This should be done prior to signing and agreeing to the General Email/Internet Security and Use Policy.

I have read and understand ’s General Email/Internet Security and Use Policy, and I understand the requirements and expectations of me as an employee.

Employee Signature: _____

Date: _____

POLICY

Personal Electronic Device Usage

Location: [INSERT LOCATION]
Effective Date: [INSERT DATE]
Revision Number: [INSERT #]

PURPOSE

recognises that employees are our most valuable asset and that they are essential contributors to our continued growth and success. Thus, we are firmly committed to employee safety and will do everything possible to prevent workplace accidents.

In production environments it is especially important that employees remain focused on their work and do not experience unnecessary distractions that could compromise safety. Studies have shown that the use of personal electronic devices (PEDs) can distract workers from what is happening around them and reduce their ability to detect and react to potential hazards. This not only leads to an increased chance of injury for the PED user, but can also jeopardise the safety of those around them.

Because of the increased risk of injury that comes with the use of PEDs, has developed this Personal Electronic Device Usage Policy, effective [INSERT DATE], to protect its employees.

SCOPE

This policy applies to all employees of and any outside contractors that may be performing work on property.

DEFINITIONS

Personal Electronic Device – includes any of the following:

- **Mobile** phone (also known as a smartphone, handheld phone or handset) – a mobile electronic device that engages in telecommunications including voice calls, text messaging/short message service (SMS) and/or email. Mobile phones also may include features like complete Internet access, games, multimedia messaging service (MMS), instant messaging (IM) service, digital audio (MP3) players, cameras, radios and satellite navigation systems. Any device that engages in these functions is included in this policy.
- Electronic device – any portable apparatus that involves user interaction. This includes, but is not limited to, laptops, satellite navigation systems, MP3 players, cameras, pagers and personal digital assistants (PDAs).
- Headset (also known as hands-free) – an extension of the mobile phone either connected to the handset via cable or wirelessly that allows the user to engage in voice communication without holding onto the mobile phone itself.

Production Area – any area that hosts the manufacture, repair, loading, unloading or storage of a product.

POLICY GUIDELINES

The following procedures apply to all employees falling under the conditions outlined above under **SCOPE.**

- PED use is banned from all production areas.
- Employees whose primary job functions require them to spend 80 per cent of their time in a production area:
  - Are not allowed to carry any PED on their person while performing work duties regardless of their location.
  - Can only use PED during break times in designated areas.

In no way does an employee's status outside of the above criteria guarantee their ability to use PED. The allowance or restriction of PED usage by employees whose primary job responsibilities take place outside of production areas will be left up to their supervisor.

EXEMPTIONS

There are a limited number of situations in which this policy may not apply

Issued Devices

Employees using company provided devices receive the following exceptions:

- Company-provided devices can be used in a restricted area if they are necessary in the performance of a company sanctioned job function that cannot be done outside of the restricted area.
- Company-provided devices can be kept on the person at all times. However, they still cannot be used in a restricted area (unless for the reason stated above).

EMERGENCY SITUATIONS

PEDs can be used in restricted areas during emergency situations if the purpose of use is to contact help or provide aid.

If you have any uncertainty or questions regarding the content of this policy, you are required to consult your supervisor. This should be done prior to signing and agreeing to the Personal Electronic Device Usage Policy.

I have read and understand 's Personal Electronic Device Usage Policy, and I understand the requirements and expectations of me as an employee. I agree to adhere to all provisions and procedures outlined in the policy, and I understand that failure to do so will result in discipline up to and including termination.

Employee Signature: _____

Date: _____

CHECKLIST | 12 STEPS TO PREPARE FOR THE GDPR

Presented by RS Risk Solutions Ltd

On 25 May 2018, the General Data Protection Regulation (GDPR) came into effect in the EU and across the United Kingdom. The GDPR replaced the Data Protection Act (DPA) and ushered in expanded rights to individuals and their data, and places greater obligations on those that process personal data.

Many of the GDPR's main concepts and principles are the same as those in the DPA, so if you complied properly with the DPA much of your approach to compliance will remain valid under the GDPR and can be a starting point to build from. However, there are new elements and significant enhancements, so you will have to do some things differently.

It is essential to plan your approach to GDPR compliance now and to gain buy-in from key people in your organisation. That is why RS Risk Solutions Ltd is here with guidance and a checklist from the Information Commissioner's Office (ICO) to help you ensure compliance.

Compliance with all the areas listed in this checklist will require you to review your approach to governance and how you manage data protection. Use the following checklist to map out which parts of the GDPR have the greatest impact on your business model, and create a plan to focus on those areas in your process.

STEP 1: AWARENESS Make sure that decision makers and key people in your organisation are aware that the law is changing. They need to appreciate the GDPR's impact.	YES	NO	ADDITIONAL NOTES
Are the key decision makers at your organisation aware that the GDPR will force you to change the way you conduct business?	☐	☐	
Do the key decision makers know how the GDPR will affect your organisation?	☐	☐	
Do the key decision makers at your organisation know what the requirements of the GDPR are?	☐	☐	
Do the key decision makers at your organisation have a plan for how you will become GDPR compliant?	☐	☐	

STEP 2: INFORMATION YOU HOLD Document what personal data you hold, where it came from and with whom you share it. You may need to organise an internal audit.	YES	NO	ADDITIONAL NOTES
Has your organisation documented what personal data you hold?	☐	☐	
Has your organisation documented where the personal data came from?	☐	☐	
Has your organisation documented with whom you share personal data?	☐	☐	
Has your organisation conducted an information audit on the personal data you hold?	☐	☐	

STEP 3: COMMUNICATING PRIVACY INFORMATION Review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.	YES	NO	ADDITIONAL NOTES
Has your organisation reviewed its current privacy notices?	☐	☐	
Does your organisation have a plan in place for making necessary changes to your privacy notices?	☐	☐	
Does your organisation know what changes need to be made in order to comply with the GDPR?	☐	☐	

STEP 4: INDIVIDUALS' RIGHTS Check your procedures to ensure they cover individuals' rights, including how you would delete personal data or provide data electronically in a commonly used format.	YES	NO	ADDITIONAL NOTES
Do your procedures cover all the rights that individuals have under the GDPR?	☐	☐	
Do your procedures allow individuals to delete their personal data?	☐	☐	
When deleting personal data, would your systems help you locate and delete data?	☐	☐	
Who will make the decisions about deletion?	☐	☐	
Do your procedures provide individuals with their data electronically and in a commonly used format?	☐	☐	

STEP 5: SUBJECT ACCESS REQUESTS Update your procedures and plan how you will handle requests within the new timescales and provide any additional information.	YES	NO	ADDITIONAL NOTES
Has your organisation updated its procedures for how you will handle subject access requests?	☐	☐	
Will your organisation be able to comply with subject access requests within one month, rather than the DPA's 40 days?	☐	☐	
Does your organisation have a plan for how it will handle subject access requests?	☐	☐	
Is your organisation ready to refuse a request, which will involve you telling the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy? Will you be able to do this without undue delay, and within one month?	☐	☐	
Is your organisation able to provide additional information upon request about subject access?	☐	☐	

STEP 6: LAWFUL BASIS FOR PROCESSING PERSONAL DATA Identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.	YES	NO	ADDITIONAL NOTES
Has your organisation identified the lawful basis for your processing in the GDPR?	☐	☐	
Does your organisation have a method to document how you process personal data?	☐	☐	
Has your organisation updated your privacy notice to reflect the lawful basis for processing personal data?	☐	☐	

STEP 7: CONSENT Review how you seek, record and manage consent, and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.	YES	NO	ADDITIONAL NOTES
Has your organisation reviewed how it seeks consent?	☐	☐	
Has your organisation reviewed how it records consent?	☐	☐	
Has your organisation reviewed how it manages consent?	☐	☐	
Does your organisation need to make any changes in its process of obtaining consent?	☐	☐	
Does your organisation have simple ways for people to withdraw consent?	☐	☐	
Is your consent separate from other terms and conditions?	☐	☐	
Can your organisation's existing consents be updated to meet the GDPR standard, meaning are they specific, granular, clear, prominent, opt-in, properly documented and easily withdrawn?	☐	☐	

STEP 8: CHILDREN Think about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.	YES	NO	ADDITIONAL NOTES
Does your organisation have a system in place to verify individuals' ages?	☐	☐	
Does your organisation have a system in place to obtain parental or guardian consent for any data processing activity?	☐	☐	

STEP 9: DATA BREACHES Make sure you have the right procedures in place to detect, report and investigate a personal data breach.	YES	NO	ADDITIONAL NOTES
Does your organisation have a procedure in place to detect a personal data breach?	☐	☐	
Now that the GDPR introduces a duty on all organisations to report certain types of data breaches to the ICO, and, in some cases, to individuals, does your organisation have a procedure in place to report a personal data breach?	☐	☐	
Does your organisation have a procedure in place to investigate a personal data breach?	☐	☐	
Does your organisation need to assess the type of personal data it holds and document when it would be required to notify the ICO or affected individuals if a breach occurred?	☐	☐	

STEP 10: DATA PROTECTION BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENTS Familiarise yourself with the ICO's code of practice on privacy impact assessments as well as the latest guidance from the Article 29 Working Party, and figure out how and when to implement them in your organisation.	YES	NO	ADDITIONAL NOTES
Is your organisation familiar with the ICO's code of practice on privacy impact assessments?	☐	☐	
Does your organisation have a strategy on how and when to implement the ICO's code of practice on privacy impact assessments?	☐	☐	
Is your organisation familiar with the latest guidance from Article 29 Working Party?	☐	☐	
Does your organisation know how and when to implement guidance from Article 29 Working Party?	☐	☐	
Does your organisation know whether it is required to undertake a data protection impact assessment (DPIA)? DPIAs are required in situations where data processing is likely to result in high risk to individuals, such as when a new technology is deployed or when a profiling operation is likely to significantly affect individuals.	☐	☐	

STEP 11: DATA PROTECTION OFFICERS Designate someone to take responsibility for data protection compliance and assess where this role will sit in your organisation's structure and governance arrangements. Consider whether you are required to formally designate a data protection officer.	YES	NO	ADDITIONAL NOTES
Has your organisation designated someone to take responsibility for data protection compliance?	☐	☐	
Has your organisation considered whether it is required to formally designate a data protection officer (DPO)? You must designate a DPO if you are a public authority, an organisation that carries out regular and systematic monitoring of individuals on a large scale, or an organisation that carries out the large scale processing of special categories of data, such as health records or information about criminal convictions.	☐	☐	
Has your organisation assessed where the data protection officer(s) will sit within your organisation's structure and governance arrangements?	☐	☐	

STEP 12: INTERNATIONAL If your organisation operates in more than one EU member state, including carrying out cross-border processing, you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you.	YES	NO	ADDITIONAL NOTES
Does your organisation operate in more than one EU member state?	☐	☐	
If your organisation has establishments in more than one EU member state or you have a single establishment that carries out processing that substantially affects individuals in other EU states, has your organisation mapped out where it makes its most significant decisions about its processing activities? This will help to determine your 'main establishment' and, therefore, your lead supervisory authority.	☐	☐	
Has your organisation determined your lead data protection supervisory authority? Use Article 29 Working Party guidelines to determine this.	☐	☐	

CHECKLIST | LAWFUL BASIS FOR PROCESSING UNDER THE GDPR

Presented by RS Risk Solutions Ltd

The General Data Protection Regulation (GDPR) replaces and mirrors the previous requirement to satisfy one of the 'conditions for processing' under the Data Protection Act. However, the GDPR places more emphasis on being accountable for and transparent about your lawful basis for processing personal data.
The six lawful bases for processing are broadly similar to the old conditions for processing. You need to review your existing processing, identify the most appropriate lawful basis and check that it applies. In many cases, it is likely the same as your existing condition for processing.

You must determine your lawful basis before you begin processing, and you should document it. Take care to get it right the first time—you should not swap a different lawful basis at a later date without good reason. If your purpose for processing changes, you may be able to continue processing under the original lawful basis if your new purpose is compatible with your initial purpose (unless your original lawful basis was consent).

To emphasise transparency and accountability, make sure that your privacy notice includes your lawful basis for processing as well as the purposes of the processing. You should also inform people upfront about which lawful basis (or bases) you rely on to process their personal data.

The six lawful bases are outlined below. Click on the title of each lawful basis for more detailed information from the Information Commissioner's Office (ICO). At least one of these must apply whenever you process personal data:

1. **Consent**—The individual has given your organisation clear consent for you to process their personal data for a specific purpose.

2. **Contract**—The data processing is necessary for a contract that you have with the individual, or because they asked you to take specific steps before entering into a contract.

3. **Legal obligation**—The data processing is necessary for your organisation to comply with the law—not including contractual obligations.

4. **Vital interests**—The data processing is necessary for your organisation to protect an individual's life.

5. **Public task**—The data processing is necessary for you to perform a task in the public's interest or for your organisation's official functions, and the task or function has a clear basis in law.

6. **Legitimate interests**—The data processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data that overrides those legitimate interests. (Note: This cannot apply if your organisation is a public authority processing data to perform your own official tasks.)

No single basis is 'better' or more important than the others—which basis is most appropriate to use will depend on your purpose and relationship with the individual. Most lawful bases require that processing is 'necessary'. If you can reasonably achieve the same purpose without the processing, you won't have a lawful basis.

Complete the following checklist to help determine which lawful basis applies. Give some thought to the wider context behind your answers and your processing activities in general. This will help you determine which lawful basis best fits the circumstances.

DETERMINING WHICH LAWFUL BASIS APPLIES	YES	NO	ADDITIONAL NOTES
We have determined what our purpose for processing is and what we are trying to achieve.	☐	☐	
We have determined whether we can reasonably achieve it in a different way.	☐	☐	
We have asked ourselves whether we have a choice over whether or not to process the data.	☐	☐	
We know whether we are a public authority.	☐	☐	
We know who our processing benefits.	☐	☐	
We have considered whether individuals would expect this processing to take place.	☐	☐	
We know our relationship with the individual.	☐	☐	
We have considered whether we are in a position of power over the individuals.	☐	☐	
We know the impact of processing on the individual.	☐	☐	
We have determined whether the individual is vulnerable.	☐	☐	
We have determined whether some of the individuals are likely to object.	☐	☐	
We are able to stop the processing at any time on request.	☐	☐	

GENERAL CONSIDERATIONS FOR DETERMINING LAWFUL BASIS	YES	NO	ADDITIONAL NOTES
We have reviewed the purposes of our processing activities and selected the most appropriate lawful basis (or bases) for each activity.	☐	☐	
We have checked that the processing is necessary for the relevant purpose, and we are satisfied that there is no other reasonable way to achieve that purpose.	☐	☐	
We have documented our decision on which lawful basis applies to help us demonstrate compliance.	☐	☐	
We have included information about both the purposes of the processing and the lawful basis for the processing in our privacy notice.	☐	☐	
Where we process special category data, we have also identified a condition for processing special category data, and have documented this.	☐	☐	
Where we process criminal offence data, we have also identified a condition for processing this data, and have documented this.	☐	☐	

If your purposes for processing data change over time or if you have a new purpose that you did not originally anticipate, you may not need a new lawful basis as long as your new purpose is compatible with the original purpose.

However, the GDPR specifically states that this does not apply to processing based on consent. You need to either get fresh consent, which specifically covers the new purpose, or find a different basis for the new purpose. If you do get specific consent for the new purpose, you do not need to show it is compatible.

In other cases, in order to assess whether the new purpose is compatible with the original purpose, ask yourself the following questions:

- Is there any link between your initial purpose and the new purpose?
- Under what context has the data been collected?
- What is your relationship to the individual?
- What kind of data processing would the individual reasonably expect from your organisation?
- What is the nature of the personal data? Is it special category? Is it criminal offence data?
- What are the possible consequences for individuals of the new data processing?
- Does your organisation have appropriate safeguards to protect the data, such as encryption or pseudonymisation?

This list of questions is not exhaustive and what you need to look at depends on your particular circumstances. As a general rule, if the new purpose is very different from the original, would be unexpected or would have an unjustified impact on the individual, it is unlikely to be compatible with your original purpose for collecting the data. You will probably need to find a new lawful basis to process the data for that new purpose.

CHECKLIST | OBTAINING CONSENT UNDER THE GDPR

Presented by RS Risk Solutions Ltd

On 25 May 2018, the General Data Protection Regulation (GDPR) came into effect in the EU and across the United Kingdom. The GDPR replaced the Data Protection Act and ushered in expanded rights to individuals and their data, and places greater obligations on businesses and other entities that process personal data.

While the GDPR includes a number of important changes regarding cyber-security and data management, one of the most important changes involves strengthening the standards of obtaining consent to process data. Failure to obtain proper consent to process data, which includes contacting individuals, risks whopping fines. The GDPR's maximum fine tops out at €20 million, or 4 per cent of global turnover, whichever is higher. The consequences are steep and there is no room for error.

But RS Risk Solutions Ltd is here with guidance from the Information Commissioner's Office (ICO) to help your business obtain consent from prospects and clients while staying compliant with the GDPR. Use the following checklist and best practice guidance to examine your own consent processes.

To comply with the GDPR's consent requirements and decide whether your existing consents meet the new, higher GDPR standard, your consent mechanisms should demonstrate the following:

- **Unbundled:** Consent requests must be separate from other terms and conditions.
- **Active opt-in:** Pre-ticked opt-in boxes are invalid—instead use unticked opt-in boxes or similar active opt-in methods, such as a binary choice given equal prominence.
- **Granular:** Give granular options to consent separately to different types of data processing wherever appropriate.
- **Named:** Name your organisation and any third parties who will be relying on the consent.
- **Documented:** Keep records to demonstrate what individuals have consented to, including what they were told, and when and how they consented.
- **Easy to withdraw:** Tell people they have the right to withdraw their consent at any time, and how to do this. It must be as easy to withdraw as it was to consent, meaning you need to have simple and effective withdrawal mechanisms in place.
- **No imbalance in the relationship:** Consent will not be 'freely given' if there is an imbalance in the relationship between the individual and data controller.

ASKING FOR CONSENT	YES	NO	ADDITIONAL NOTES
We have checked that consent is the most appropriate lawful basis for processing.	☐	☐	
We have made the request for consent prominent and separate from our terms and conditions.	☐	☐	
We ask people to positively opt in.	☐	☐	
We do not use pre-ticked boxes or any other type of consent by default.	☐	☐	
We use clear, plain language that is easy to understand.	☐	☐	

ASKING FOR CONSENT, continued	YES	NO	ADDITIONAL NOTES
We specify why we want the data and what we are going to do with it.	☐	☐	
We give granular options to consent to independent processing operations.	☐	☐	
We have named our organisation and any third parties.	☐	☐	
We tell individuals they can withdraw their consent.	☐	☐	
We ensure that the individual can refuse to consent without harm.	☐	☐	
We do not make consent a precondition of service.	☐	☐	
If we offer online services directly to children, we only seek consent if we have age-verification and parental-consent measures in place.	☐	☐	

Can I use existing Data Protection Act consents?

Remember that, although you are not required to automatically 'repaper' or refresh all existing Data Protection Act (DPA) consents in preparation for the GDPR, it is important to check your processes and records in detail to be sure existing consents meet the GDPR standard.

If your existing DPA consents ***do not*** meet the GDPR's high standards or are poorly documented, you will need to seek new GDPR-compliant consent.

How should I write a consent request?

Consent requests need to be prominent, concise, easy to understand and separate from any other information, such as general terms and conditions. Use the following best practices as guidance:

- Keep your consent requests separate from other general terms and conditions, and clearly direct people's attention to them.
- Use clear, straight-forward language.
- Adopt a simple style that your intended audience will find easy to understand.
- Avoid technical jargon and confusing terminology, such as double negatives.
- Use consistent language and methods across multiple consent options.
- Keep your consent requests concise and specific, and avoid vague or blanket wording.

What information should I include in my consent requests?

Consent requests should, at a minimum, include the following:

- The name of your organisation and the names of any third parties who will rely on the consent
- Why you want the data
- What you will do with the data
- That people can withdraw their consent at any time

What methods can I use to obtain consent?

Whatever method you use must meet the standard of an unambiguous indication by clear, affirmative action. This means you must ask people to actively opt in. Examples of active opt-in mechanisms include the following:

- Signing a consent statement or paper form
- Ticking an opt-in box on paper or electronically
- Clicking an opt-in button or link online
- Selecting from equally prominent yes or no options
- Choosing technical settings or preference dashboard settings
- Responding to an email requesting consent
- Answering yes to a clear oral consent request

RECORDING CONSENT	YES	NO	ADDITIONAL NOTES
We keep a record of when and how we got consent from the individual.	☐	☐	
We keep a record of exactly what the individual was told at the time.	☐	☐	

How should I record consent?

You must have an effective audit trail of how and when consent was given, so you can provide evidence if challenged. Good records will also help you monitor and refresh consent as appropriate. You must keep good records that demonstrate the following:

- **Who consented:** The name of the individual or other identifier
- **When they consented:** A copy of a dated document or online record that includes a timestamp; or, for oral consent, a note of the time and date that was made at the time of the conversation
- **What they were told at the time:** A master copy of the document or data capture form containing the consent statement in use at that time, along with any separate privacy policy, including version numbers and dates matching the date consent was given. If consent was given orally, your records should include a copy of the script used at that time.
- **How they consented:** For written consent, a copy of the relevant document or data capture form. If consent was given online, your records should include the data submitted as well as a timestamp to link it to the relevant data capture form. If consent was given orally, you should keep a note of this made at the time of the conversation—it does not need to be a full record of the conversation.
- **Whether they have withdrawn consent:** And, if they have, when they withdrew their consent.

MANAGING CONSENT	YES	NO	ADDITIONAL NOTES
We regularly review consent to check that the relationship, the processing and the purposes have not changed.	☐	☐	
We have processes in place to refresh consent at appropriate intervals, including any parental controls.	☐	☐	
We consider using privacy dashboards or other preference management tools as a matter of good practice.	☐	☐	

MANAGING CONSENT, continued	YES	NO	ADDITIONAL NOTES
We make it easy for individuals to withdraw their consent at any time and publicise how to do so.	☐	☐	
We act on withdrawals of consent as soon as we can.	☐	☐	
We do not penalise individuals who wish to withdraw consent.	☐	☐	

How should I manage consent?

Your obligations do not end when you get consent. You should view consent as a dynamic part of your ongoing relationship of trust with individuals, not a one-off compliance box to tick and file away. To reap the benefits of consent, you need to offer ongoing choice and control. It is good practice to provide preference management tools like privacy dashboards to allow people to easily access and update their consent settings. Find more ICO guidance on these tools by clicking here.

You should keep your consents under review. You will need to refresh them if anything changes—for example, if your processing operations or purposes evolve, the original consent may not be specific or informed enough. If you are in doubt about whether the consent is still valid, you should refresh it.

You should also consider whether to automatically refresh consent at appropriate intervals. How often it is appropriate to do so will depend on the particular context, including people's expectations, whether you are in regular contact and how disruptive repeated consent requests would be to the individual. If in doubt, the ICO recommends you consider refreshing consent every two years. If you are not in regular contact with individuals, consider sending occasional reminders of their right to withdraw consent and how to do so.

How should I manage the right to withdraw consent?

The GDPR gives people a specific right to withdraw their consent. You will need to ensure that you put proper withdrawal procedures in place. As the right to withdrawal is at any time, it is not enough to provide an opt-out only by reply. Individuals must be able to opt out at any time they choose, on their own initiative. It must also be as easy to withdraw consent as it was to give it. This means the process of withdrawing consent should be an easily accessible one-step process. If possible, individuals should be able to withdraw their consent using the same method as when they gave it.

It is good practice to publicise both online preference management tools and other ways of opting out, such as customer service phone numbers. You should bear in mind that not everyone is comfortable with technology or has access to the internet. If someone originally gave consent on paper or in person, it may not be enough to offer only an online opt-out.

It is also good practice to provide both anytime opt-out mechanisms, such as privacy dashboards, and opt-out by reply to every contact. This could include an unsubscribe link in an email or an opt-out phone number, address or web link printed in a letter.

If someone withdraws consent, you should stop the processing immediately, particularly in an online automated environment. However, in other cases, you may be able to justify a short delay while you process the withdrawal. You must include details of the right to withdraw consent in your privacy notices and consent requests. It is best practice to also include details of how to withdraw consent.

For more information on cyber best practices, contact the insurance professionals at RS Risk Solutions Ltd by calling 0333 003 0676 or visiting www.rsrisk.solutions today.

CHECKLIST | LEGITIMATE INTERESTS UNDER THE GDPR

Presented by RS Risk Solutions Ltd

In order for your organisation to process individuals' personal data, you must have a lawful basis (or bases). One of these bases is legitimate interests, which the Information Commissioner's Office (ICO) defines as:

'[Data processing which] is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.'

Out of the six lawful bases, legitimate interests is the most flexible, yet that does not mean that it is the most appropriate. It is likely to be most appropriate when you use people's data in ways they would reasonably expect and have a minimal privacy impact, or where there is a compelling justification for the processing.

If you choose to rely on legitimate interests, you are taking on extra responsibility for considering and protecting people's rights and interests. The legitimate interests can be your own interests or the interests of third parties—a wide range of interests may be legitimate interests. The GDPR specifically mentions use of client or employee data, marketing, fraud prevention, intra-group transfers, or IT security as potential legitimate interests, but this is not an exhaustive list. If you don't need consent under the Privacy and Electronic Communications Regulations (PECR), you can rely on legitimate interests for marketing activities if you can show that how you use people's data is proportionate, has a minimal privacy impact, and that people would not be surprised or likely to object. See the ICO's guide to PECR for more information on when you need consent for electronic marketing.

Before you decide that legitimate interests is the most applicable basis, complete a legitimate interests assessment (LIA). An LIA is a type of risk assessment based on the specific context and circumstances that will help you ensure that your processing is lawful. LIAs can be broken down into a three-part test:

1. **Purpose test:** Are you pursuing a legitimate interest?
2. **Necessity test:** Is the processing necessary for that purpose?
3. **Balancing test:** Do the individual's interests override the legitimate interest?

Complete the three-part LIA checklist and the general considerations checklist below to determine whether you can rely on the legitimate interests clause to process personal data under the GDPR.

Legitimate Interests Assessment:

STEP 1: CONDUCTING A PURPOSE TEST	YES	NO	ADDITIONAL NOTES
We know why we want to process the data and what we are trying to achieve.	☐	☐	
We understand who benefits from the processing and in what way.	☐	☐	
We have investigated whether there are any wider public benefits to the processing and how important those benefits are.	☐	☐	
We have evaluated what the impact would be if we couldn't go ahead with the processing.	☐	☐	
We have scrutinised whether our use of the data would be unethical or unlawful in any way.	☐	☐	

STEP 2: CONDUCTING A NECESSITY TEST	YES	NO	ADDITIONAL NOTES
We have determined that our processing helps to further the legitimate interest that we have identified.	☐	☐	
We agree that our plans are a reasonable way to go about processing individuals' data.	☐	☐	
We have considered whether there is a less intrusive way to achieve the same result.	☐	☐	

STEP 3: CONDUCTING A BALANCING TEST	YES	NO	ADDITIONAL NOTES
We have identified the nature of our relationship with the individuals.	☐	☐	
We have determined whether any of the data is particularly sensitive or private.	☐	☐	
We have considered whether people would expect us to use their data in this way.	☐	☐	
We are happy to explain to people how we use their data.	☐	☐	
We have considered whether some people are likely to object or find it intrusive.	☐	☐	
We have considered the possible impact on the individual and how big that impact would be.	☐	☐	
We have determined whether we process any children's data.	☐	☐	
We have considered whether any of the individuals are vulnerable in any way.	☐	☐	
We have examined whether we can adopt any safeguards to minimise the impact our processing would have on individuals.	☐	☐	
We have examined whether we can offer an opt-out to individuals.	☐	☐	
Does the impact of our processing override our interests?	☐	☐	

Once you have undertaken the three-part LIA, be sure to keep a record of it and the outcome. There is no standard format for this, but it's important to record your thinking to help show you have proper decision-making processes in place and to justify the outcome.

Keep your LIA under review and refresh it if there is a significant change in the purpose, nature or context of the processing.

If you are not sure about the outcome of the balancing test, it may be safer to look for another lawful basis. Legitimate interests will often not be the most appropriate basis for processing that is unexpected or high risk. If you do rely on legitimate interests to process data, remember that you must tell people in your privacy notice that you are relying on legitimate interests and explain what those interests are.

If you want to process the personal data for a new purpose, you may be able to continue processing under legitimate interests as long as your new purpose is compatible with your original purpose. In this case, the ICO still recommends that you conduct a new LIA, as this will help you demonstrate compatibility.

If you rely on legitimate interests for direct marketing, the right to object is absolute and you must stop processing when someone objects.

After conducting your three-part LIA, complete the general considerations checklist below to identify anything else that may prevent you from relying on the legitimate interests clause to process data.

GENERAL CONSIDERATIONS FOR USING LEGITIMATE INTERESTS	YES	NO	ADDITIONAL NOTES
We have checked that legitimate interests is the most appropriate basis for processing data.	☐	☐	
We understand our responsibility to protect the individual's interests.	☐	☐	
We have conducted an LIA and kept a record of it to ensure that we can justify our decision.	☐	☐	
We have identified the relevant legitimate interests.	☐	☐	
We have checked that the processing is necessary and there is no less intrusive way to achieve the same result.	☐	☐	
We have done a balancing test and are confident that the individual's interests do not override our legitimate interests.	☐	☐	
We only use individuals' data in ways they would reasonably expect, unless we have a very good reason.	☐	☐	
We are not using people's data in ways they would find intrusive or that could cause them harm, unless we have a very good reason.	☐	☐	
If we process children's data, we take extra care to make sure we protect their interests.	☐	☐	
We have considered safeguards to reduce the impact where possible.	☐	☐	
We have considered whether we can offer an opt-out.	☐	☐	
If our LIA identifies a significant privacy impact, we have considered whether we also need to conduct a data protection impact assessment (DPIA).	☐	☐	
We keep our LIA under review, and repeat it if circumstances change.	☐	☐	
We include information about our legitimate interests in our privacy notice.	☐	☐	

CHECKLIST | International Data Transfers

Presented by RS Risk Solutions Ltd

The General Data Protection Regulation (GDPR) imposes restrictions on the transfer of personal data outside the European Union to other countries or international organisations. These restrictions are in place in order to ensure that individuals' personal data is protected and secure under the GDPR regardless of where their data is shared.

Transfers may be made when the EU Commission has decided that a third country, a territory or one or more specific sectors in the third country, or an international organisation ensures an adequate level of protection.

In the absence of such a decision, you may complete a transfer of personal data outside the European Union if the organisation receiving the personal data has provided at least one of the adequate safeguards listed in Table 1.

To ensure that your organisation is compliant with the GDPR in the international transfer of personal data, complete the following checklists.

#1: HAS THE ORGANISATION RECEIVING THE PERSONAL DATA PROVIDED ONE OF THE FOLLOWING ADEQUATE SAFEGUARDS?	YES	NO	ADDITIONAL NOTES
A legally binding agreement between public authorities or bodies	☐	☐	
Binding corporate rules (agreements governing transfers made between organisations within a corporate group)	☐	☐	
Standard data protection clauses in the form of template transfer clauses adopted by the EU Commission	☐	☐	
Standard data protection clauses in the form of template transfer clauses adopted by a supervisory authority and approved by the EU Commission	☐	☐	
Compliance with an approved code of conduct approved by a supervisory authority	☐	☐	
Certification under an approved certification mechanism as provided for in the GDPR	☐	☐	
Contractual clauses agreed and authorised by the competent supervisory authority	☐	☐	
Provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority	☐	☐	

In the absence of an EU Commission decision or the appropriate safeguards listed in Table 1, a transfer, or set of transfers, may be made when the transfer meets at least one of the conditions laid out in Table 2.

#2: DOES THE PERSONAL DATA TRANSFER MEET ONE OR MORE OF THE FOLLOWING QUALIFICATIONS?	YES	NO	ADDITIONAL NOTES
Made with the individual's informed consent	☐	☐	
Necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request	☐	☐	
Necessary for the performance of a contract made in the interests of the individual between the controller and another person	☐	☐	
Necessary for important reasons of public interest	☐	☐	
Necessary for the establishment, exercise or defence of legal claims	☐	☐	
Necessary to protect the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent	☐	☐	
Made from a register which under UK or EU law is intended to provide information to the public (and which is open to consultation by either the public in general or those able to show a legitimate interest in inspecting the register)	☐	☐	

Even when there is no EU Commission decision authorising transfers to the country in question, if it is not possible to demonstrate that the individual's rights are protected by adequate safeguards (such as in Table 1) and none of the exemptions apply (such as in Table 2), the GDPR provides that personal data may still be transferred outside the EU. Such transfers are permitted only when the transfer meets all the conditions laid out in Table 3 below.

#3: FOR TRANSFERS WITH NO EU COMMISSION DECISION AUTHORISING THE TRANSFER, THEY MUST MEET ALL THE FOLLOWING CRITERIA	YES	NO	ADDITIONAL NOTES
The data transfer is not being made by a public authority in the exercise of its public powers	☐	☐	
The data transfer is not repetitive (similar transfers are not made on a regular basis)	☐	☐	
The data transfer involves data related to only a limited number of individuals	☐	☐	
The data transfer is necessary for the purposes of the compelling legitimate interests of the organisation (provided such interests are not overridden by the interests of the individual)	☐	☐	
The data transfer is made subject to suitable safeguards put in place by the organisation (in the light of an assessment of all the circumstances surrounding the transfer) to protect personal data	☐	☐	

In these cases, your organisation is required to inform the relevant supervisory authority of the transfer and provide additional information to the individuals.

CHECKLIST | PERSONAL DATA BREACHES UNDER THE GDPR

Presented by RS Risk Solutions Ltd

The General Data Protection Regulation (GDPR) introduces a duty on all organisations to report certain types of personal data breaches to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible.

A personal data breach refers to a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

In 2017, 46 per cent of all UK organisations experienced at least one cyber-security breach or attack, according to the government's cyber-security breaches survey.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must inform those individuals without undue delay. You should ensure that you have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individuals. You must also keep a record of any personal data breaches, regardless of whether you are required to notify.

Under the GDPR, an organisation may be fined up to €20 million (roughly £16 million) or 4 per cent of its annual turnover—whichever is higher—for violating the basic principles related to data security. What's more, if your organisation fails to notify the relevant supervisory authority of a breach, it can result in a fine of up to €10 million or 2 per cent of your annual turnover, depending on which is higher.

Use this checklist to comply with the GDPR's rules surrounding personal data breaches:

PREPARING FOR A DATA BREACH	YES	NO	ADDITIONAL NOTES
We know how to recognise a personal data breach.	☐	☐	
We understand that a personal data breach isn't only about loss or theft of personal data.	☐	☐	
We have prepared a response plan for addressing any personal data breaches that occur.	☐	☐	
We have allocated responsibility for managing breaches to a dedicated person or team.	☐	☐	
Our staff knows how to escalate a security incident to the appropriate person or team in our organisation to determine whether a breach has occurred.	☐	☐	

RESPONDING TO A DATA BREACH	YES	NO	ADDITIONAL NOTES
We have in place a process to assess the likely risk to individuals as a result of a breach.	☐	☐	
We know who is the relevant supervisory authority for our processing activities.	☐	☐	
We have a process to notify the Information Commissioner's Office (ICO) of a breach within 72 hours of becoming aware of it, even if we do not have all the details yet.	☐	☐	
We know what information we must give the ICO about a breach.	☐	☐	
We have a process to inform affected individuals about a breach when it is likely to result in a high risk to their rights and freedoms.	☐	☐	
We know we must inform affected individuals without undue delay.	☐	☐	
We know what information about a breach we must provide to individuals, and that we should provide advice to help them protect themselves from its effects.	☐	☐	
We document all breaches, even if they don't all need to be reported.	☐	☐	

HOW TO REPORT A DATA BREACH	COMPLETED
Contact the relevant supervisory authority of a breach within 72 hours of your organisation becoming aware of it.	☐
Directly contact individuals affected by a breach if it is likely to result in a high risk to their rights and freedoms. (Note: A 'high risk' means the threshold for notifying individuals is greater than notifying the relevant supervisory authority.)	☐
Complete a breach notification, which should contain the following information: • The categories and number of individuals affected by the breach • The categories and number of personal data records affected by the breach • The name and contact details of the data protection officer (if your organisation has one) or an additional contact where more information can be obtained • A detailed description of the potential consequences of the data breach • A detailed description of what measures your organisation has taken or will take to address the data breach • A detailed description of the measures your organisation has taken or will take to mitigate any possible adverse effects to either itself or the individuals affected	☐

NOTIFICATION REQUIREMENTS OF A PERSONAL DATA BREACH: