WinckworthSherwood

Demystifying the GDPR


WinckworthSherwood

Contents

Introduction

The General Data Protection Regulation (GDPR), due to come into force on 25 May 2018, will impose significant new burdens on organisations across Europe, including a substantial amount of additional reporting requirements and increased fines and penalties. The UK Government recently announced that after Brexit the UK will continue to adopt a similar standard for data protection as set out in the GDPR. This guide sets out the key changes under the GDPR and the considerations and actions to take in relation to personal data.

OUR GDPR TEAM

TONI VITALE
HEAD OF REGULATION, DATA & INFORMATION
020 3735 1934
tvitale@wslaw.co.uk

JON BALDWIN
PARTNER, REGULATION, DATA & INFORMATION
020 7593 0384
jbaldwin@wslaw.co.uk

ANDREW YULE
PARTNER, EMPLOYMENT
020 7593 5089
ayule@wslaw.co.uk

ROBERT PAYDON
PARTNER, DISPUTE RESOLUTION
020 7593 5022
rpaydon@wslaw.co.uk

LOUISE LAWRENCE
SENIOR ASSOCIATE, EMPLOYMENT
020 7593 5082
llawrence@wslaw.co.uk

THERESA KERR
SENIOR ASSOCIATE, EDUCATION
020 7593 5154
tkerr@wslaw.co.uk

Why implement new legislation?

The GDPR is not intended to restrict the processing of personal data, but rather align it to the modern digital world and ensure that such processing is done in a way that **protects the data subject's rights**. For example, many organisations outsource services to third parties (e.g. payroll or training services), use cloud hosting services (rather than onsite data racks) and engage with data subjects (e.g. through training/surveys) to collect and analyse workforce demographic, knowledge and expertise. Such behaviour will need to be reviewed (but not necessarily restricted) in light of the upcoming GDPR.

Who will be affected?

The quick answer is every organisation in the UK that handles personal data. These new data protection rules will apply both to the personal data of individuals living in the EU and also to the export of personal data to countries outside the EU. Most importantly for people here, it covers UK businesses, despite any changes that might occur in the 'post-Brexit' era.

GDPR applies to data controllers (people who specify how and why personal data is processed) and data processors (those who carry out the processing). Controllers must ensure that their processors comply with the legislation and the processors must also keep records of their processing activities. The new law means that both parties face a more stringent level of liability than they do under the existing law.

The key changes

- Changes to how consent can be obtained from data subjects for the use of their data. For example, data subjects have to explicitly 'opt in' to allowing their data to be shared, and it must be made clear what their data is being used for
- **Data subjects have new rights**, such as data portability and the right to be forgotten, requiring all organisations to understand exactly where all data on individuals is held
- **Data must only be used for the purpose it was gathered for** and should be **deleted** when it is no longer needed for that purpose
- **Sanctions over sharing data outside the EEA will be strengthened**. This requires organisations to ensure adequacy decisions or appropriate privacy safeguards are in place with organisations holding data outside the EEA. This impacts cloud and outsourced services.
- All new and existing **staff must have suitable training and awareness**, as well as additional sources of guidance and support when required
- Conducting **Data Protection Impact Assessments** (DPIA) in order to design data privacy into any new systems and processes will often be mandatory. E.g. if new technology is being deployed, where there is processing on a large scale of 'sensitive personal data', or if profiling is being performed which is likely to have an impact on individuals
- Some organisations will need to appoint a **Data Protection Officer**
- **Data breaches** must be reported to the ICO within 72 hours of the breach
- **A new principle of 'accountability'** puts the burden on those at executive management and board level for compliance, requiring them to produce and maintain documents that demonstrate what actions have been taken to achieve compliance.

What is the scope of the GDPR?

Many of the existing core concepts under the Data Protection Act 1998 (DPA) are reflected in the GDPR. Familiar concepts of personal data, data controllers and data processors are broadly similar in both the DPA and the GDPR. Currently there is a very broad definition of 'processing' under the DPA and this captures the retrieval, management, transmission, destruction and retention of personal data. This will continue to be the case under the GDPR as well.

If your organisation is not in the EU, you will still have to comply with the GDPR. Non-EU organisations that do business in the EU with EU data subjects' personal data should designate a representative in the EU, as a point of contact for supervisory authorities (who are responsible for ensuring compliance with the GDPR) and data subjects.

What's new? Legal rights of Data Subjects	
DPA 1998	*GDPR/new Data Protection Bill 2017*
Under the current law a Data Subject can request a copy of their data (Subject Access Request) on payment of a nominal fee and has a common law right of erasure or rectification of their personal data.	Under the GDPR, these rights are explicit and no longer require a fee. In addition, there is a right to have personal data extracted in an electronic portable format that will allow switching between different service providers. There are new rights to erase data too (if it is no longer needed).

Under the GDPR, **personal data** now includes information relating to a living person, who can be identified directly or indirectly by such information (e.g. name, ID number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic or social identity of that person). Under the GDPR, **sensitive personal data** (which has a higher threshold of protection) will include genetic data, biometric data and data concerning sexual orientation, in addition to the previous categories such as race/ethnic origin, trade union membership, health and criminal records.

The first step is to understand the flow of personal data both internally and externally. Both UK and international organisations this will need to understand how data flows within the organisation and outside particularly when the data crosses international borders. For example, where organisations outsource a particular function, perhaps data hosting (which includes HR data) and/or management of its payroll service, such services will be subject to the more stringent obligations under the GDPR. Moreover, non-EU affiliates using shared resources and/or centralised functions are likely to be directly affected by the GDPR given its further territorial scope.

Organisations should review their existing contracts in light of the GDPR, assessing current policies and procedures in place in light of the flow of data across the business. Going forward, the increased obligations and liability under the GDPR should be considered in future negotiations to ensure an adequate risk allocation with suppliers. In general, businesses should expect more lengthy and difficult negotiations with suppliers as they try to address their new exposure under the GDPR.

What is a privacy notice?

The **transparency requirements** under the GDPR require organisations to provide individuals (i.e. employees and customers) with extensive information about how their personal data is collected, stored and used. This information must be easily accessible, transparent and presented using clear and plain language. In practice, this means that organisations will need to include more information in their privacy policies, as well as retaining more detailed records of their data processing activities in relation to their employees, customers and third parties.

A gear shift in risk

The huge increase in fines (from £500,000 in the UK to the greater of €20million or 4% of global annual turnover) places significantly additional risk on organisations. The GDPR will allow users to claim damages in the instance of data loss as a result of unlawful processing, including collective redress, the equivalent of a US-style class action lawsuit.

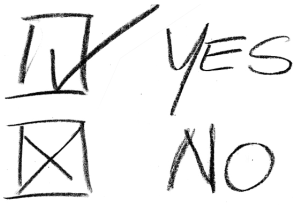
Lastly, it is worth remembering the **additional costs** that can be incurred as well. Similar to a breach of the DPA, a breach of the GDPR could expose organisations to substantial internal resource spent on responding to requests for information, enforcement notices, internal and external press releases and minimising any negative PR. You should consider reviewing your 24 hour data breach response plan (as set out in our '12 Steps To Include In A Data Breach Response Plan').

What's new? Notifying breaches	
DPA 1998	*GDPR/new Data Protection Bill 2017*
Currently the notification of breaches to the ICO is effectively voluntary.	The GDPR introduces a new obligation to notify breaches to the ICO within 72 hours and in some cases data subjects will have to be notified too.

Under the GDPR, organisations will be required to **report a personal data breach within 72 hours** to the Information Commissioner. In line with the accountability requirements, all data breaches must be recorded along with details of actions taken. Organisations should appoint a data breach response team, outline a response plan and set out a detailed reporting procedure in the updated privacy policy detailing how, when and to whom data subjects should report data breaches. Organisations should also review any reporting requirements and assistance set out in outsourced services agreements.

Can consent be relied on?

Similar to the DPA, the GDPR also requires the processing of personal data to be in accordance with certain conditions of processing. One of these conditions, which is often relied on, is **the data subject's consent**, with wording in privacy notices and/or employment contracts confirming the individual's consent to the processing of their personal data.



Under the GDPR, **consent must be unambiguous**. Consent to process sensitive personal data must be explicit, however, consent to process other types of personal data does not need to be explicit. Consent must, however, still be specific, informed and active: silence or inactivity is not sufficient.

Consent must be freely given and individuals must be able to withdraw consent (without detriment). Entering into a contract, or receiving a service, should not be 'tied' to the user giving consent to the processing of data which is not, in fact, necessary for the service to be delivered. Organisations must also seek separate consents for separate processing operations. There is a presumption that these types of forced or omnibus consent mechanisms will not be valid: organisations will need to redesign consent mechanisms so as to present genuine and granular choice for consent to be valid.

What's new? Marketing consents	
DPA 1998	*GDPR/new Data Protection Bill 2017*
Under current law an opt-out can be relied on by marketers for gaining marketing consent (for example, tick here if you don't wish to receive offers, etc).	Under the GDPR, marketing consent must be explicit and in a form of: • time limited opt-in • in plain language • easy way to opt-out and to say no to profiling If consent can't be proved, a company could face a big fine under the GDPR and an Enforcement Order to stop processing customer data

Processing does not need to be based on consent: other bases for processing still exist, including contractual necessity, compliance with a (Member State or EU) legal obligation and where the processing is necessary for the legitimate interests of the controller (or another organisation) provided that these interests are not overridden by the data protection rights of the individual. Processing in order to prevent fraud, for direct marketing and for network security are all cited as examples of processing carried out for a legitimate interest. Sharing data (both employee and customer) within a group of undertakings may also be necessary for a legitimate interest.

Public bodies are, however, not able to rely on this legitimate interests justification.

The Information Commissioner has recently published draft guidance on consent under the GDPR. This sets out that it is unlikely that an employer will be able to show that an employee has given valid consent under the GDPR (i.e. that it has been freely given) and employers should rely on one of the other conditions for processing.

The need to document your data processing

Controllers and processors must keep and make available to supervisory authorities very comprehensive records of data processing which in turn requires organisations to start work on detailed data mapping exercises to determine what data is collected, how and why, where it is stored, who has access to it and whether there is a legal justification to process it.

Lawful basis for processing

The GDPR will require organisations to take a much closer look at each purpose of data processing to ensure that there is a valid justification, particularly as the 'bucket' justifications of consent and legitimate interests will be much narrower.

The GDPR sets out six lawful basis for processing data. Unless an exemption applies at least one of these will apply in all cases. It is possible for more than one to apply at the same time. One of the new requirements for Privacy Notices is that you must set out in the Privacy Notice which Lawful basis you are relying on.

Consent

A controller must be able to demonstrate that consent was given. Transparency is key: consents given in written declarations which also cover other matters must be clearly distinguishable, and must be intelligible, easily accessible and in clear and plain language. Consent is defined as any freely given, specific, informed and unambiguous indication of the data subject's wishes – either by a statement or by a clear affirmative action.

Consent will be necessary to process children's data

Parental consent will be required for the processing of personal data of children under age 16. EU Member States may lower the age requiring parental consent to 13. In the draft Data Protection Bill recently published by the UK Government, the UK has adopted this option to reduce the age of consent to 13.

Legitimate interests

This involves a balancing test between the controller (or a third party's) legitimate interests and the interests or fundamental rights of and freedoms of the data subject – in particular where the data subject is a child. The privacy policy of a controller must inform data subjects about the legitimate interests that are the basis for the balancing of interests. "Direct marketing" is recognised as a possible legitimate interest (as an alternative to consent).

The balancing test

- Identify your legitimate interest - what is the purpose of the processing and why is it important?
- Carry out a necessity test - is there another way of achieving your legitimate interest? If the answer is no, then it is necessary.
- Carry out a balancing test

    - Does the data subject's right override the legitimate interest?
    - Consider the nature of the processing, it's impact and what mitigation you can put in place.
    - What possible negative impacts for privacy could there be

Contractual necessity

Personal data may be processed if the processing is necessary in order to enter into or perform a contract with the data subject (or to take steps prior to entering into a contract).

Compliance with legal obligation

Personal data may be processed if the controller is legally required to perform such processing (e.g. reporting of race or ethnic origin or gender pay data).

Vital Interests

Personal data may be processed to protect the 'vital interests' of the data subject (e.g. in a life or death situation it is permissible to use a person's medical or emergency contact information without their consent).

Public Interest

Personal data may be processed if the processing is necessary for the performance of tasks carried out by a public authority or private organisation acting in the public interest.

Can I process sensitive personal data?

Sensitive personal data means information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health, sexual life, criminal history and allegations. The GDPR adds the following new additional categories: **genetic data, biometric data and sexual orientation.** To process sensitive personal data one of the following should apply – however please note that:

(a) More than one of the criteria below can apply at the same time
(b) Data controllers need to establish a lawful basis for processing any personal data (see previous section Lawful basis for processing) - and in addition if they are processing sensitive personal data they must also establish that at least one of the criteria below applies:

1. **Explicit consent** of the data subject (which can be withdrawn).
2. **Employment Law** – if it is necessary for employment law or social security or social protection.
3. **Vital Interests** – e.g. in a life or death situation where the data subject is incapable of giving consent.
4. **Charities, religious organisations and not for profit organisations** – to further the interests of the organisation on behalf of members, former members or persons with whom it has regular contact such as donors.
5. **Data made public by the data subject** – it needs to have been made public 'manifestly'.
6. **Legal claims** – where it is necessary for the establishment, exercise or defence of legal claims or for the courts acting in this judicial capacity.
7. **Reasons of substantial public interest**, where the processing is proportionate to the aim pursued and the rights of individuals are protected.
8. **Medical Diagnosis or treatment** – where the processing is necessary for medical treatment by health professionals including assessing work capacity or the management of health or social care systems.
9. **Public Health** – where the processing is necessary for reasons of public health e.g. safety of medical products.
10. **Historical, statistical or scientific purposes** where it is necessary for statistical purposes in the public interest for historical, scientific research or statistical purposes.

More accountability, governance, and resourcing

Achieving readiness for the GDPR will require much **wider engagement right across an organisation** to drive the necessary change.

There is **a new focus on accountability**: businesses must be able to demonstrate they have complied with the data processing principles, for example through the use of Privacy Impact Assessments or showing compliance with Codes of Conduct or Certifications.

Role of the Data Protection Officer

What's new? – Data Protection Officer (DPO)	
DPA 1998	*GDPR/new Data Protection Bill 2017*
Currently 4 out of 10 member states in the EU require a DPO to be appointed for most organisations but this was implemented under local laws rather than the EU legislation. It was not required in the UK but was mandatory in Germany.	Under the GDPR, controllers and processors must appoint a DPO if they carry out processing involving the 'regular and systematic monitoring of data subjects on a large scale' or if they process sensitive personal data or data relating to criminal convictions and offences 'on a large scale', or if they are a public authority.

The Data Protection Officer's role is to inform and advise the organisation about its obligations to comply with the GDPR, monitor compliance, including managing internal data protection activities, provide training to staff, advise on data protection impact assessments and conduct internal audits and they should:

- **Be the first point of contact** for the supervisory authority
- **Directly report** to the highest management level of the controller or processor
- **Not be given instructions** on how to carry out duties and can't be dismissed for carrying out duties
- **Can combine duties** if no conflict of interest
- **Be contactable** by data subjects
- Be provided with **necessary resources**

What is privacy by design and default?

The GDPR requires data controllers to implement appropriate technical and organisational measures to protect data subjects' rights. This can include anonymising or pseudonymisation of data and restricting the amount of personal data processed, the access granted and/or any retention period. Coupled with this, there is an accountability principle under the GDPR requiring organisations to be able to demonstrate how they comply with the GDPR.

This requires a cultural shift in the approach to personal data protection going forward rather than something that can be done in isolation or as a one-off. Organisations should encourage a focus on awareness and training in relation to the new GDPR requirements. Documenting current processing activities on an ongoing basis, conducting data privacy impact assessments where necessary and auditing third party providers to ensure that the GDPR requirements are being met are all sensible steps for organisations to take.

What's new? CCTV	
DPA 1998	*GDPR/new Data Protection Bill 2017*
The ICO has a code of conduct for CCTV users which recommends a sign is erected notifying visitors they are being recorded.	Companies should revisit the signs to ensure full transparency – for example does the sign state that automatic number plate recognition software is used and list all the purposes the data collected will be used for?

What about my contracts with suppliers and partners?

Organisations should review their existing contracts in light of the GDPR, assessing current policies and procedures in place in light of the flow of data across the business. Going forward, the increased obligations and liability under the GDPR should be considered in future negotiations to ensure an adequate risk allocation with suppliers. In general, businesses should expect more lengthy and difficult negotiations with suppliers as they try to address their new exposure under the GDPR.

What's new? Contracts with data processors and joint controllers	
DPA 1998	*GDPR/new Data Protection Bill 2017*
The current law did not make contracts compulsory but it was regarded as good practice.	The GDPR requires contracts to be entered into and stipulates eleven mandatory topics which must be included. If organisations fail to do this by May 2018 both controllers and processors can be fined.

What must be included?

- Processor must process data only on instructions of controller
- People authorised to access data are subject to confidentiality
- Ensure security of processing
- Assist the controller in complying with data subjects rights (where possible)
- Assist the controller with regard to security measures, breach reporting and DPIAs

What are the additional data subject rights?

Right of portability

Data subjects will have the right to request that their personal data be provided to them (or a third party) in a machine readable portable format free of charge. Organisations should consider how and where the personal data is held and if such data can be easily transferred in a safe, secure manner without impacting the usability of such data by the data subject. The organisation will need to comply with such requests without undue delay, and in any event within one month.

Right to be forgotten (right to erasure)

Data subjects have the right to request the removal or erasure of their personal data, such as if it is no longer necessary to process their data, the individual objects to such processing and/or the individual withdraws consent. Not only will organisations need to comply with such requests but they will also need to ensure that any third party with whom the data was shared also deletes such data.

Data subject access requests

Under the GDPR the right of data subjects to request information about the personal data processed by organisations remains largely the same. However, under the new regime organisations must respond without undue delay and in any case within one month of receipt of the request. Additionally, the £10 fee for making a request will be abolished which is likely to lead to a greater number of requests. It is estimated that 25% of requesters at present withdraw or do not pursue their request when asked to fill in a form and pay the current £10 fee. Organisations will need to consider if they have sufficient resources to deal with a 25% increase in the volume of data subject access requests.

The new data subject rights may present practical issues for organisations, especially where personal data is spread across multiple or complex systems. Organisations will need to update the relevant policies and procedures to reflect the new GDPR requirements. You should review existing procedures in place when responding to data subject access requests to ensure the new time scales can be met.

Other rights:

- The right to be informed
- The right to restrict processing
- Rights in relation to automated decision-making and profiling
- The right to rectification
- The right to object

Next steps

Please see overleaf our Checklist and our GDPR Action Plan which will provide a useful starting point when considering your approach to GDPR compliance.

GDPR Checklist

①	**Raise awareness** – Your management and taff should be made aware that the law is changing. They need to know enough to make good decisions about what you need to do to implement GDPR. Add data protection to your risk register if you have one. **Decide who will be responsible for data protection in your organisation** – Someone in your organisation, or an external data protection advisor, has to take responsibility for compliance with data protection legislation and have the knowledge and authority to do this effectively.
②	**Map your data** – If you do not know what personal data you hold and where it came from you will need to organise an audit of your systems and departments to find out. This means all personal data including employees and volunteers, service users, members, donors and supporters and more. You should document your findings because you must keep records of your processing activities. You should also record if you share data with any third parties.
③	**Identify and document your 'lawful basis' for processing data** – To legally process data under GDPR you must have a 'lawful basis' to do so. For example it is a lawful basis to process personal data to deliver a contract you have with an individual. There are a number of different criteria that give you lawful basis to process and crucially, different lawful basis give different right to individuals. Understand and document your lawful basis for processing data.
④	**Check your processes meet individuals' new rights** –GDPR will give people more rights over their data. For example GDPR gives someone the right to have their personal data deleted. Would you be able to find the relevant data and who would be responsible for making sure that happened? Get to know the eight rights and have the systems in place to be able to deliver on each of them. **Know how you will deal with 'subject access requests'** –Individuals have the right to know what data you hold on them, why the data is being processed and whether it will be given to any third party. They have the right to be given this information in a permanent form (hard copy). This is known as a 'subject access request'or "SAR". Your organisation needs to be able to identify a SAR, find all the relevant data and comply within one month of receipt of the request. Under GDPR the time limit for responding to SARs is reduced to from 40 days to 30 days and the £10 fee is abolished.
⑤	**Review how you get consent to use personal data** –If you rely on consent as your lawful basis for processing personal data, then you need to review how you seek and manage consent. Under GDPR consent must be freely given, specific and easily withdrawn. You can't rely on pre-ticked boxes, silence or inactivity to gain consent instead people must positively opt-in.
⑥	**Build in extra protection for children** – Many organisations support children and young people and GDPR brings in special protection for childrenildrenPR brings in DPR says children under 16 cannot give consent (although this will be reduced to 13 in the UK) so you may have to seek consent from a parent or guardian. You will need to be able to verify that person giving consent on behalf of a child is allowed to do so and any privacy statements will need to be written in language that children can understand.
⑦	**Update your Policies & Notices** **Privacy Notices** - You must always tell people in a concise, easy to understand way how you intend to use their data. Privacy notices are the most common way to do this. You may well already have privacy notices but they will all need to be updated. Under GDPR, privacy notices must give additional information such as how long you will keep data for and what lawful basis you have to process data. **Policies** – Have clear, practical policies and procedures on information governance for staff to follow, and monitor their operation.

⑦

Data Retention & Disposal – Ensure you update your data retention policy and inform all data subjects how long you will retain data. When disposing of records and equipment, make sure personal information cannot be retrieved from them.

Data sharing – Be sure you are allowed to share information with others and make sure it is kept secure when shared. Formal written agreements will now be required and these include GDPR required clauses.

Websites – Control access to any restricted area. Make sure you are allowed to publish personal information (including images) on your website/social media.

CCTV – Inform people what it is used for and review retention periods. If your CCTV cameras cover public areas, you may require a SIA licence. Ensure you have the correct signage on display and a suitable policy in place.

Training – Train staff and trustees on the basics of information governance, where the law and good practice need to be considered, and know where to turn for advice.

⑧

Update your contracts to deal with processing by others – Recognise when others are processing personal information for you make sure they do it securely. You will need to ensure your contracts are updated to include the GDPR required clauses and put in place an audit program to supervise them. Consider also how you select suppliers. There must be a written contract which imposes these obligations on processors:

Processors must:

1. Follow instructions of the controller
2. Ensure their personnel are under a duty of confidence.
3. Keep the personal data secure
4. Allow Controllers to consent to sub-contractors.
5. Flow down obligations to sub-contractors (but remain responsible for actions of the sub-contractor(s)
6. Assist the controller when individuals exercise their rights to access, rectify, erase or object to processing of data.
7. Assist the controller with privacy impact assessments
8. Assist the controller with security and data breach obligations and notify the controller of any personal data breach
9. Return or delete data at the end of the agreement (but can keep a copy)
10. Demonstrate compliance with these obligations and submit to audits
11. Inform the controller if their instructions would breach the law

⑨

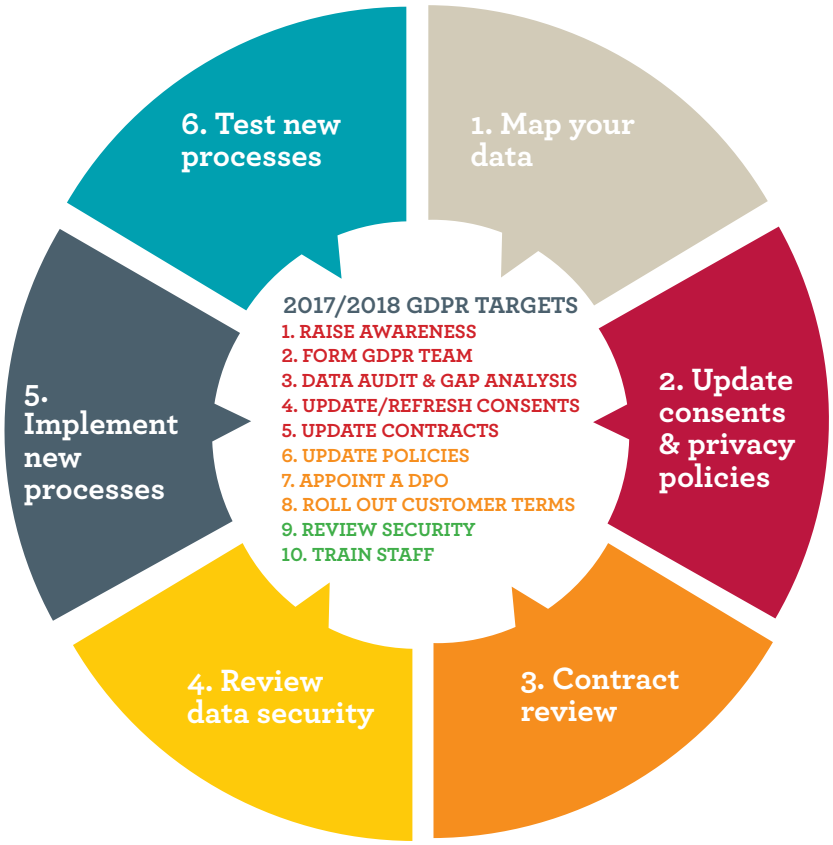
Get ready to detect, report and investigate personal data breaches - A data breach is a breach of security leading to 'accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data'. You will need to have the right procedures in place to detect, investigate and report a breach. The GDPR introduces a duty to report certain types of data breaches to the ICO and in some cases to the individuals concerned. You need to be able to demonstrate that you have appropriate technical and organisational measures in place to protect against a breach.

⑩

Build data protection into your new projects - Privacy by design means building data protection into all your new projects and services. It has always been good practice, but GDPR makes privacy by design an express legal requirement. To achieve this, data protection impact assessments should be undertaken where new technology is being deployed, where profiling may significantly affect individuals or sensitive categories of data will be processed on a large scale. Clarify who will be responsible for carrying out impact assessments, when you will use them and how to record them.

GDPR 2018 Action Plan

Winckworth Sherwood



1. MAP YOUR DATA

Questions to ask:

1. Where is my data?
2. Where does my data come from?
3. Why are we collecting it?
4. Where is data held?
5. Where does it go around the company?
6. Who has access to the data? What are their skills, clearance & training?
7. How sensitive is the data (personal, sensitive, anonymous)?
8. Which 3rd parties is it shared with? How is it transferred? What agreements and contracts do you have with processors?
9. How is data transferred overseas?
10. Where are your Cloud servers?
11. What encryption is used?
12. Does your data leave the EEA? If so who 'exports' it and who receives it?

A. If your data leaves the EU what method is used now (e.g. model clauses)?

B. Would binding corporate rules work for your organisation?

2. UPDATE CONSENTS & PRIVACY POLICIES

Consider & review:

1. What consents do you have and are they GDPR compliant?
2. Customer journeys and terms and conditions
3. Marketing, competitions and promotions
4. Fair processing notices
5. Privacy policies
6. Website terms
7. Who is your current DPO and can they be your GDPR DPO if you need one?

3. CONTRACT REVIEW

Consider & review:

1. Supplier contracts from data processors
2. Contracts where you are the processor
3. Joint data controller contracts
4. Prioritise contracts according to risk (not value, necessarily)
5. Upgrade IT to add functionality

(i) Keep a log of all consents (e.g. web, social media, digital, contract)
(ii) Offer a 'right to be forgotten'
(iii) Allow objections to profiling
(iv) Allow 'data portability'

6. Also consider: A. "Privacy By Design" built into each system change
B. "Data Protection Impact Assessments" for major system overhauls

4. REVIEW DATA SECURITY

1. Are there adequate firewalls and virus protections?
2. Is there a clear password policy? Is it enforced?
3. Is there a procedure in place for data breach management?
4. Who is responsible for it?
5. Do all staff understand the procedure?
6. Include response, notification process recovery and damage limitation
7. Include risk assessment for the consequences of the breach?
8. What investigative process is triggered to ascertain the cause of the breach and if response can be improved?
9. Test breach management procedure with a 'mock' breach?
10. What do you do with your data when you aren't using it?
11. Review storage and data elimination/ destruction policies

5. IMPLEMENT NEW PROCESSES

1. New consent formats and refresh old consents
2. Stop relying on consent where you should not do so (e.g. employees)
3. New fair processing notices (both for customers and employees)
4. New privacy policies
5. New data retention policy
6. New DSAR process & training
7. Processes to implement new rights (e.g. erasure, correction, portability)
8. New breach reporting process
9. New model clause contracts (if needed)
10. Refresh staff training

6. TEST NEW PROCESSES

Test and train:

1. Breach reporting
2. DSARs
3. Exercising new rights (e.g. rectification/ erasure)
4. Re-review customer terms and processes

How can Winckworth Sherwood's GDPR team assist you?

1	**Raise awareness**	Helping you prepare and deliver: Board presentations Training FAQs	Target: January 2018
2	**Data audits**	Data Audits Surveys Mapping *Please ask for our sample audit questionnaires*	Target: January 2018
3	**Update privacy processes/DPO appointment**	Reviewing & updating: Fair processing notices Website terms Privacy policies DPO Appointments: *Please ask for our guide to DPOs including a job specification*	Target: February 2018
4	**Customer & consent review**	Reviewing consents & whether they should be refreshed, customer journeys, customer terms and marketing (including competitions and promotions)	Target: February 2018
5	**Contract review**	Supplier/third party contract review New contract terms Amending existing contracts Negotiation training for procurement teams	Target: February 2018
6	**Map overseas data transfers**	Review international data transfers Consider Binding Corporate Rules Review use of model clauses	Target: March 2018
7	**HR processes**	Review HR & internal policies and procedures, including fair processing notices, privacy policies and contracts – avoiding reliance on consent	Target: April 2018
8	**DSAR & breach reporting**	Review subject access request processes DSAR training Review how other rights will be implemented Review breach reporting processes	Target: April 2018
9	**Security review**	Review & update security processes & policies Guidance on what to do in the first 24 hours after a breach Training on how to avoid reputation issues post breach Review	Start: January 2018 Complete April 2018
10	**DPIA support**	Conducting Data Protection Impact Assessments Assessing whether a DPIA is necessary *Please ask for our DPIA assessment checklists*	Start: January 2018 Complete early 2018

Contact us

OUR GDPR TEAM

TONI VITALE
HEAD OF REGULATION, DATA & INFORMATION
020 3735 1934
tvitale@wslaw.co.uk

JON BALDWIN
PARTNER, REGULATION, DATA & INFORMATION
020 7593 0384
jbaldwin@wslaw.co.uk

ANDREW YULE
PARTNER, EMPLOYMENT
020 7593 5089
ayule@wslaw.co.uk

ROBERT PAYDON
PARTNER, DISPUTE RESOLUTION
020 7593 5022
rpaydon@wslaw.co.uk

LOUISE LAWRENCE
SENIOR ASSOCIATE, EMPLOYMENT
020 7593 5082
llawrence@wslaw.co.uk

THERESA KERR
SENIOR ASSOCIATE, EDUCATION
020 7593 5154
tkerr@wslaw.co.uk

Winckworth Sherwood

Winckworth Sherwood