KEMP LITTLE

#KLdemystify Data Protection

May 2020

Data protection toolkit

Part 1: What is data protection and why is it so important?

KEMP LITTLE

What is the difference between privacy and data protection?

Privacy is a socially-agreed-on respect for private & family life, home and correspondence.

Data protection is part of a fundamental right to **privacy** - but on a more practical level. It is a system of data processing practices which apply to information capable of identifying an individual for the protection of privacy.

Data protection is about keeping data safe and using data fairly and responsibly. It is about building trust between people and organisations, recognising **an individual's** right to have control over their personal information when it is held by others and striking a balance between those individual rights and the wider interests of society.

Does data protection apply to me?

Yes, if you process information about people outside of a domestic setting data protection laws will apply to you. Processing is very broadly defined and covers almost anything you can do with data including collecting, recording, storing or transmitting information.

Senior managers of UK companies should read this toolkit to gain a practical overview of your company's **current data protection** obligations.

General Data Protection Regulation

- **What is the GDPR?**

The **GDPR*** is an **EU Regulation** (supplemented in the UK by the **Data Protection Act 2018**). It was brought in to:

- Consolidate data privacy laws across Europe
- Protect the rights and freedoms of EU citizens in an increasingly data-driven world

- **What is the scope of GDPR?**

GDPR applies to:

- Processing by companies **established** in the UK and **EEA** (regardless of whether processing occurs in Europe or not)
- Companies established **outside** the EEA offering goods or services to **data subjects** in the UK or EEA
- Monitoring the behaviour of EEA or UK data subjects in Europe

If you work with companies in the UK or EEA they ma also expect you to comply with or maintain GDPR standards. GDPR has become a first-class privacy standard and is often used as a template for new privacy laws worldwide as part of an increasing trend of protecting privacy rights in law; GDPR compliance will give you a business advantage, mitigate regulatory risks and build consumer confidence.

*See the glossary of jargon at the end

Who are the key stakeholders?

- Senior Management: Board/ Executive Committee (or similar)
- Head of Compliance
- Head of IT
- Head of HR
- General Counsel

What does the Data Protection Toolkit cover?

Practical advice covering the following areas:

Part 1: What is Data Protection and why is it so important? Overview of your main data protection obligations under GDPR

Part 2: Implementing data protection How can I be a top ten compliant organisation?

Part 3: Keeping personal data safe Understand the importance of data security

Part 4: Accountability Understand you are subject to an accountability principle, meaning you must be able to demonstrate your compliance

Part 5: What happens if we do something wrong? Understand that GDPR non-compliance can be very costly

Part 6: UK GDPR Understand how Brexit will affect your data protection obligations

- **Key dos and don'ts**
- **How Kemp Little can help you**
- **Glossary of jargon**
- **Other useful resources**

Five questions every board should be asking

What does GDPR mean for business process?

It is essential to build good data protection compliance into business processes at every stage and every level (aka **data protection by design and default**).

A critical starting point is to conduct an initial **top to bottom review of all business activities** and associated data processing activities to create a **data flow map.**

How can we educate employees?

The focus on **accountability** (see Part 4 below) and the level of scrutiny GDPR places on organisations makes an ongoing training programme for **all staff** essential.

Employees must understand how to protect the data they deal with in their role (the dos *and* the dont's), how to comply with your company policies and what to do if they discover a data breach. Training must be tailored and practical and don't forget to keep a record.

Do we need to invest in technology?

In appropriate technology yes! But what?

Invest in **privacy-enhancing technology** (PET) that will assist with compliance by minimising personal data use, maximising data security, efficiency, and empower individuals. Choose technology which is helpful and flexible enough to be tailored to the needs of your business. First class solutions might offer perfect compliance but if they are too complicated or too time consuming they will probably never be used to their full potential.

There are numerous data management tools available which can help you with record keeping, managing user consents and data subject requests, investigation of data breaches and a vast range of data security options including encryption, anti-virus and firewall software together with virtual private networks and two factor authentication (see security below).

Are we collecting data that we don't need?

Collecting and accessing excess personal information can be common practice. Streamlining your processing to what you strictly require will help you to comply with GDPR data minimisation requirements, and reduce your overall exposure.

Am I covered against any GDPR-related fines?

Board members should check the company insurance cover.

Fines for criminal conduct are uninsurable in the UK. It is unlikely that companies can insure against GDPR fines although it is currently untested and it will depend on the type of breach. Either way, the legal costs and liabilities associated with a data breach are insurable and without cover the personal costs could be significant.

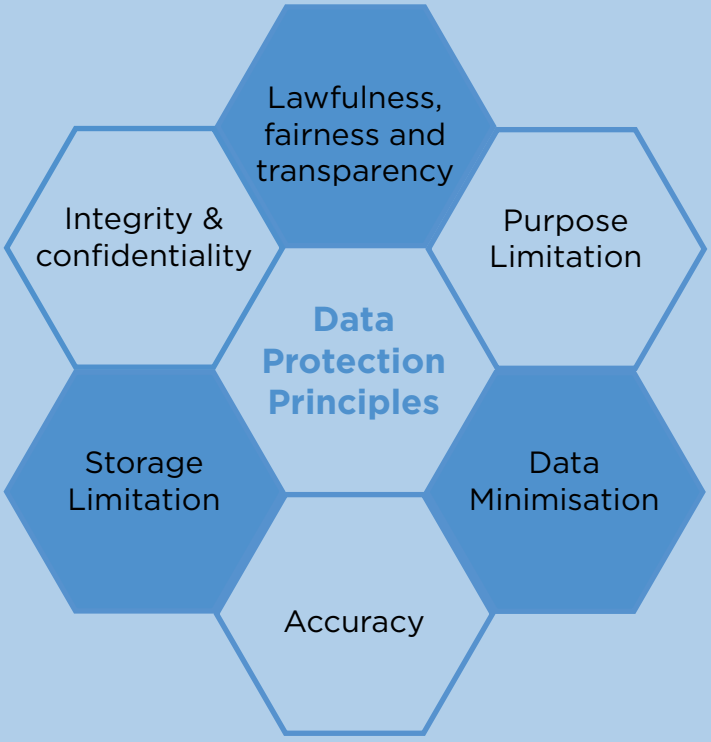
Data protection toolkit

Part 2: Implementing data protection

KEMP LITTLE

Data Protection Principles

Data must be obtained lawfully and you must tell the individual exactly how you will use their data in a privacy notice
Keep to your word!



Why do you need the data? Be specific!

You must justify the amount of data collected, so make sure you only collect the minimum data you need

Only store accurate and up-to-date data

Don't keep archived documents for decades! Retain data only for as long as necessary and then erase

Keep data secure

Can you prove to the ICO that you are compliant with all these principles?

How are these principles translated into practice?

- **Lawfulness, fairness and transparency**

Explain what you are doing and why. This can be achieved by providing a **privacy notice** to those individuals whose data you collect. Being as clear as possible from the outset with individuals will build trust.

You need a **lawful basis** for processing. If things change, keep individuals informed.

- **Only process data for the purposes you collected it for**

If you collected personal data for data reporting, then don't use it to send newsletters!

- **Data minimisation**

Only collect data that you need. For example, if you only need contact details and a CV for recruitment purposes, then you should not also collect financial details if it is not necessary.

- **Accuracy**

Keep the data up to date. If an employee informs you that their bank account number has changed ensure that there is a process in place to inform the payroll provider so that payments are made into the correct account and update the record.

- **Storage limitation**

Why keep the data of that job applicant who was interviewed in 2014? Delete it: agree retention periods and stick to them!

- **Integrity and Confidentiality**

Make sure personal information is kept securely (**special category personal data** must be treated with extra care), encrypted (wherever possible) and that strict access controls are in place.

Policies and procedures

You should adopt a **Privacy Policy** (aka Data Protection Policy) that establishes the **principles, standards and controls** for the protection of personal data within your company and applicable to all personnel handling personal data and those with decision-making authority over those processes. Note that the Privacy Policy sets out your internal rules on how to process data, a privacy notice explains to the affected individuals what you're doing with data and why.

In addition, these policies will help to maintain data protection within your organisation and, importantly to demonstrate **accountability.** Once you have agreed the company policy you may want to draft a separate **procedure** which gives staff clear and practical guidance on the steps they must follow to comply with the policy.

Security	Accountability
Information security (InfoSec) policy	Data protection be design policy
Information risk management	Data breach policy
Anonymisation policy	Record retention policy
Bring your own device policy	Data subject rights policy
Business contnuity plan and disaster recovery policy	Data protection impact assessment (DPIA) policy

Example of independent controllers

A UK company (Co A) with global operations sends staff to deprived areas of the world to set up new projects and they employ the services of an emergency medical response company (Co B) as a precaution. In an emergency, personal data is transferred from Co A to Co B and on to Co C, a local private medical team to provide the response.

Co B is co-ordinating with Co C and controlling the rescue effort and independently determining how the personal data is used.

Example of joint controllers

A luxury car company teams up with a designer fashion brand to host a co-branded promotional event. The companies decide to run a prize draw at the event. They invite attendees to participate in the prize draw by entering their name and address into their prize draw system, which is shared with both companies. After the event, the companies send prizes to the winners.

The companies will be joint controllers of the personal data, because they decided the purposes and means of the processing together.

Do you have a DPO? Do you need one?

- **What is a Data Protection Officer?**

The concept of a DPO is not a new one but the role is more prominent under GDPR. The DPO monitors internal compliance, advises on your data protection obligations and acts as a contact point for data subjects and the ICO.

The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level.

The DPO may have other roles within the company and you can outsource the function e.g. **Kemp Little KLick DPO.**

- **Is a DPO mandatory?**

A DPO is only mandatory where:

1. Processing is carried out by a **public authority**

2. The core activities of your processing operations require regular and **systematic monitoring of data subjects on a large scale**

3. Your core activities consist of processing **special categories of data on a large scale or personal data relating to criminal convictions and offences**

It is good practice and **highly recommended to have a DPO** even where there is no legal requirement. A DPO will help you stay on top of privacy compliance and make sure it doesn't get lost on a 'to do' list.

Contracting with third parties

- **Is your company sharing personal data with a third party?**

Where **data controllers** share data with **data processors** there must be a **data processing agreement** in place.

Who is the data controller? The data controller **decides the purposes and means of the data handling** activity.

Who is the data processor? The data processor **processes the data on behalf** of the data controller and on their written instructions.

Examples of data processing agreements include outsourcing payroll/IT support/document archiving/travel booking/cloud storage etc.

In some cases the relationship is more complex and the customer and the supplier will both be data controllers. If the parties independently determine the purpose and the means of processing as part of the service delivery the parties will be **independent controllers.** If the parties jointly determine the purpose and the means of the processing they will be **joint controllers.**

- **What about the contract?**

If there is a processor relationship, then there must be a data processing agreement (DPA or data protection clauses

annexed to the services agreement).

As a minimum, the DPA must contain the following processor obligations:

- Comply with applicable data protection laws
- Only act on the controller's documented instructions
- Make no international data transfers without approval (or subject to agreed safeguards)
- Ensure staff are bound by confidentiality
- Implement appropriate security meaures
- Lists the subject matter, duration, nature of processing and types of personal data and data subjects involved
- Not sub-contract without approval
- Assist the controller with data subject requests
- Assist the controller with data breach notification
- Assist the controller with DPIAs
- Delete or return data at the end of the contract
- Assist the controller with audits

If there is a **controller to controller relationship** you will, at the very least, want contractual certainty that the third party will comply with the applicable data protection laws but where a joint controller relationship exists the parties are **joint and severally liable** and must **allocate their compliance responsibilities in a 'transparent manner' including responsibility for subject access requests and privacy notices.**

But there are many more provisions you could include which would ensure co-operation between the parties to ensure data protection compliance and which would give the controller more peace of mind.

- **What other practical steps should you take?**
  - **Data audit** to understand the **complex data flows** within your organisation and, the **volume of personal data** (and special category data) and the location of data (important for record keeping, **DSARs** (see below) and data breach reporting)
  - **New vendor/supplier management risk assessment** – do you have an onboarding procedure to assess the extent of data processing in new supplier relationships?
  - **Supplier sub-contracts** – are the processor obligations replicated and how is this dealt with in the overall risk positions in the contract?
  - **Due diligence** – is your InfoSec team confident that the supplier you have chosen is capable of complying with data protection laws?
  - Assessment of existing **privacy processes and documentation** – are they compliant with GDPR?
  - **New process risk assessment** – do you assess the risks of new data processing activities (see **DPIAs** below)?

Do you carry out DPIAs?

A **Data Protection Impact Assessment** is designed to help you analyse, identify and minimise the data protection risks of a project.

It is key to your **accountability obligations** and helps you to assess and demonstrate how you comply with data protection laws.

The DPIA should help you minimise risk and determine whether the level of risk is acceptable rather than eliminating the risk all together.

- **What types of processing automatically require a DPIA?**

Systematic and extensive automated processing (i.e. without human input) including profiling where the outcome could have a significant effect on the individual

E.g. profiling job candidates and online behavioural advertising activities using cookies to identify users and show personalised ads based on their profile

Large scale use of special category data or criminal conviction data

E.g. processing of patient health data by pharmaceutical companies in clinical studies

Large scale public monitoring

E.g. facial recognition used at airport security and CCTV at train stations to prevent crimes

Can you accommodate all the data subject rights?

The GDPR sets out individual rights which include:

Access: You must provide individuals with a copy of each item of personal data you hold about them

E.g. an employee contemplating litigation against their employer may make a **'data subject access request'** (aka **DSAR**)

Rectification: You must amend or update their personal data where it is inaccurate

E.g. if an employee tells you they have moved house, your records must be updated

Stop direct marketing

Restrict process

Information

Access

Rectification

Erasure

Portability

Object

Erasure: If individuals no longer wish to have their personal data stored by you, they can ask you to **delete the information** you hold about them (aka the **right to be forgotten**)

E.g. a customer sends this email: "Please delete all my data – I am no longer a customer!"

Objection to processing: Individuals have an absolute right to stop their data being used for direct marketing or can challenge your legitimate business interests

E.g. a customer no longer want to receive your newsletter

Restriction of processing: You may have to **limit the processing** of an individual's data in some specific circumstances

E.g. you no longer need the personal data but the individual needs your company to keep it in order to establish, exercise or defend a legal claim

Portability: Allows individuals **to move, copy or transfer personal data** easily from one supplier to another in a safe and secure way, without affecting its usability

E.g. transmission of data from your customer databaseto another data controller

Information: Individuals have the right to be informed about the collection and use of their personal data

E.g Information provided through privacy notices, banners, podcasts, videos

How do you make sure you can accommodate data subjects when they look to exercise those rights?

- Ensure your IT systems allow you to quickly (within the 1 month time limit) identify and isolate data relating to a specific individual
- **Automated responses** are recommended where possible due to the time limits and the obligation to provide responses **free of charge**
- **Secure authentication** will be required to identify data subjects
- **Privacy policies and privacy notices must be updated** to reflect the data subject rights and the record keeping requirements
- **Employees must be trained** to respond to data subject requests – companies can extend the time limits or refuse requests in certain circumstances

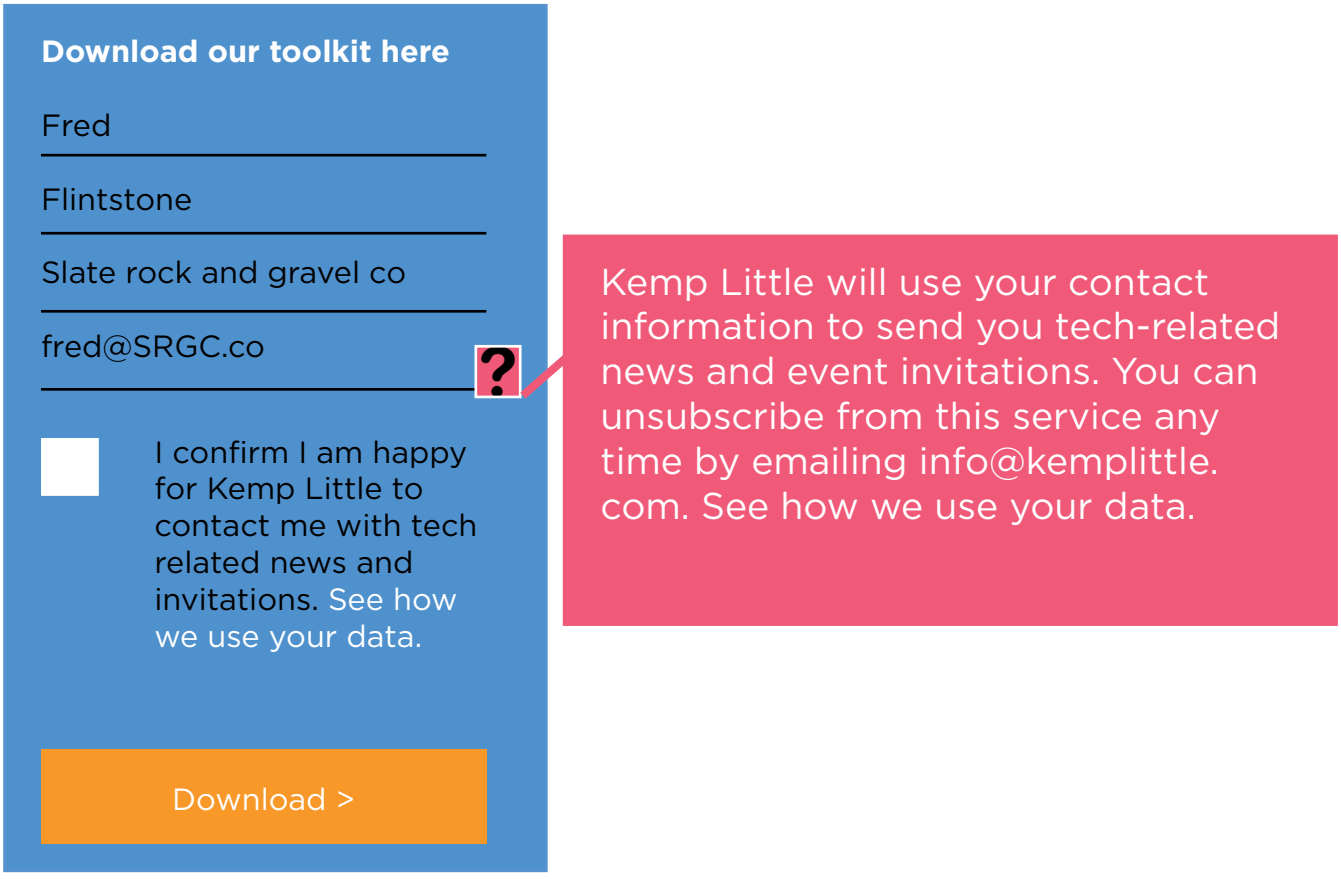
Collecting valid consent for marketing

Consent is central to the rules on **direct marketing.**

Organisations will generally need an individual's consent before you can send unsolicited marketing texts, emails or make any automated marketing calls according to **PECR**. Please note that this also applies to indirect marketing activities such as sending newsletters (not just hard sell) and to charities. The rules are less strict on B2B marketing.

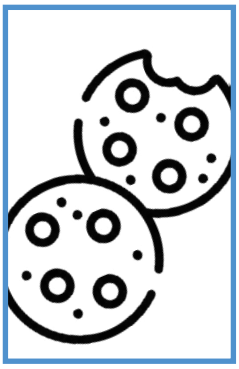
Valid Consent must be:

- **Freely given**; this means giving people genuine ongoing choice and control over how you use their data
- **Obvious** and require a **positive action to 'opt in'**
- **Prominent, unbundled** from other terms and conditions, **concise** and **easy to understand** and user-friendly
- **Easy to withdraw** at any time



Consent may also be required where you have no other **lawful basis** for processing personal data or special category personal data (which requires the more onerous **explicit consent**), for example where you want to share data in an unexpected or potentially intrusive way and you cannot rely on **legitimate business interests.** Due to the unreliable nature of consent it is best avoided where there is an alternative option.

Cookies and behavioural targeting



Behavioural targeting is a technique used in online advertising and publishing, where data from visitor browsing habits (e.g. web site visits) are used to display relevant ads and offers and improve campaign effectiveness.

Websites use cookies for behavioural targeting and other purposes including:

- Remembering what's in an online shopping basket
- Supporting users logging in to websites
- Analysing website traffic
- Tracking users' browsing behaviour

Cookies are regulated by PECR and subject to strict standards of consent and transparency under GDPR. The ICO has published guidance on the use of cookies and similar technologies.

Hurry up! You should take prompt action to review your use of cookies and other web-based technologies and make the necessary remedial changes!

Data protection toolkit

Part 3: Keeping personal data safe

KEMP LITTLE

Security of processing

The **GDPR** and the **DPA 2018** require data controllers and data processors to implement **appropriate technical and organisational measures** which take into account the '**state of the art', cost, type of data processing** and the **rights and freedoms of data subjects.**
Put simply, each company must:

1. **Map its data flows** and assess the volume and types of data processing undertaken to identify the risks to individuals if those processes were compromised.
2. **Audit the security measures in place** including technical solutions (e.g. network security, firewall, anti-virus software, email security, **multi-factor authentication** and anti-**malware** etc), the physical security arrangements for your building and your policies on staff transporting data and accessing data remotely (especially important if you have employees working from home)
3. Decide on an appropriate **information security strategy** based on the range of technical solutions available and the relative cost of implementation
4. Document your strategy in an **Info Sec policy** and complimentary policies such as a **BYOD** policy.

Be cautious with new products

The use of video conferencing technology soared with the outbreak of the coronavirus pandemic and raised some serious security concerns, e.g. 'Zoombombing' of uninvited participants joining a Zoom conference call.

There are lots of practical ways to keep your personal data secure, here are just a few suggestions:

- **Strong IT team** with enough information security expertise to manage the volume and complexity of personal data processed by your organisation (or access to additional external expertise)
- **Good 'depth of defence' cybersecurity strategy** for implementing layers of security, e.g. infrastructure security, systems security, software and platform security, risk management and incident response
- **Consistent approach to security across all departments and effective communication between teams**
- Due diligence of suppliers and supply contract terms to ensure secure processing/sub-processing
- Adequate safeguards for all international data transfers outside of the UK/EEA
- Practical Info Sec policies and procedures which staff understand and are prepared to work with rather than work around
- Staff training to ensure that new staff know what to do and existing staff receive refresher training
- Encourage reporting of technical difficulties (e.g. homeworkers with no access to virtual private network (VPN) tools) to minimise security risks
- Ensure the board leads by example, follows company policies and doesn't expect special treatment

What is a data breach?

> "A personal data breach is a **breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.**"

Data breaches are happening all around us. They can be a **deliberate, malicious** and/or **highly technical attack**, for example:

- **Theft** of hard copy documents, a USB stick, a laptop or a mobile phone
- **Unauthorised access** to an email account or IT system (by a sophisticated cyber hacker or someone who finds a password on a 'Post-it note')
- A **disgruntled employee** who copies a list of customer contacts before they leave your employment

But many more data breaches are caused by **human error.** Here are some examples of how the **accidental or careless behaviour** of your own staff can cause a data breach:

- Sending an **email to the wrong person**
- Sending a **bulk invite by email using 'to' or 'cc'**, instead of the 'bcc' field
- **Leaving documents, laptops or mobile phones on public transport**
- Posting **unencrypted documents by standard post**
- Disposing of sensitive documents in a **communal recycling bin**
- Leaving **filing cabinets unlocked** in areas with general access

Hotel chain **Marriott** disclosed a **major data breach in March 2020**: the **second in 2 years!**

Hackers obtained the contact details and other personal data of up to 5.2M guests: useful information for a **spear-phishing** campaign. Experts suggest that Marriott n**eglected to implement standard security measures such as multi-factor authentication and guest account monitoring.**

To help minimise staff related data breaches it is important to develop a positive information security culture within your organisation.

Don't blame staff for making the wrong decisions. Train staff to trust their instincts; if an email looks suspicious encourage them to report it as a potential **phishing** scam.

Make reporting easy. If the identity of whistle-blowers is kept confidential and you give feedback to prove that reports are taken seriously, staff are more likely to inform you of potential problems.

Don't panic! Remember the saying "act in haste and repent at leisure"?

Vicarious liability for employee actions?

You can follow expert advice and make sure that your security is fully compliant with data protection requirements, but you can never fully control the actions of your staff.

Morrisons Supermarkets came under fire after an employee copied payroll data for nearly 100K employees onto a USB stick, which he later posted on a file sharing website and sent to the media. The employee was found criminally liable and jailed for 8 years. The ICO investigated and decided that Morrisons was not itself in breach of the data protection law and the Supreme Court has recently decided that Morrisons wasn't **vicariously liable for the actions of its employee.**

On the facts of this case, the employee was not acting in the ordinary course of his duties. Whilst the result will be a relief for Morrisons, there is still a risk of UK employers being held vicariously liability for data breaches caused by employees in some scenarios.

The case highlights the need to have in place adequate safeguards to try to prevent such attacks from insiders and a means of recovering your financial loss where possible, e.g. contractual indemnities and insurance.

Data protection toolkit

Part 4: Accountability

KEMP LITTLE

What is accountability?

Accountability is one of the key data protection principles - it makes you responsible for complying with the GDPR and requires you to **demonstrate your compliance.**

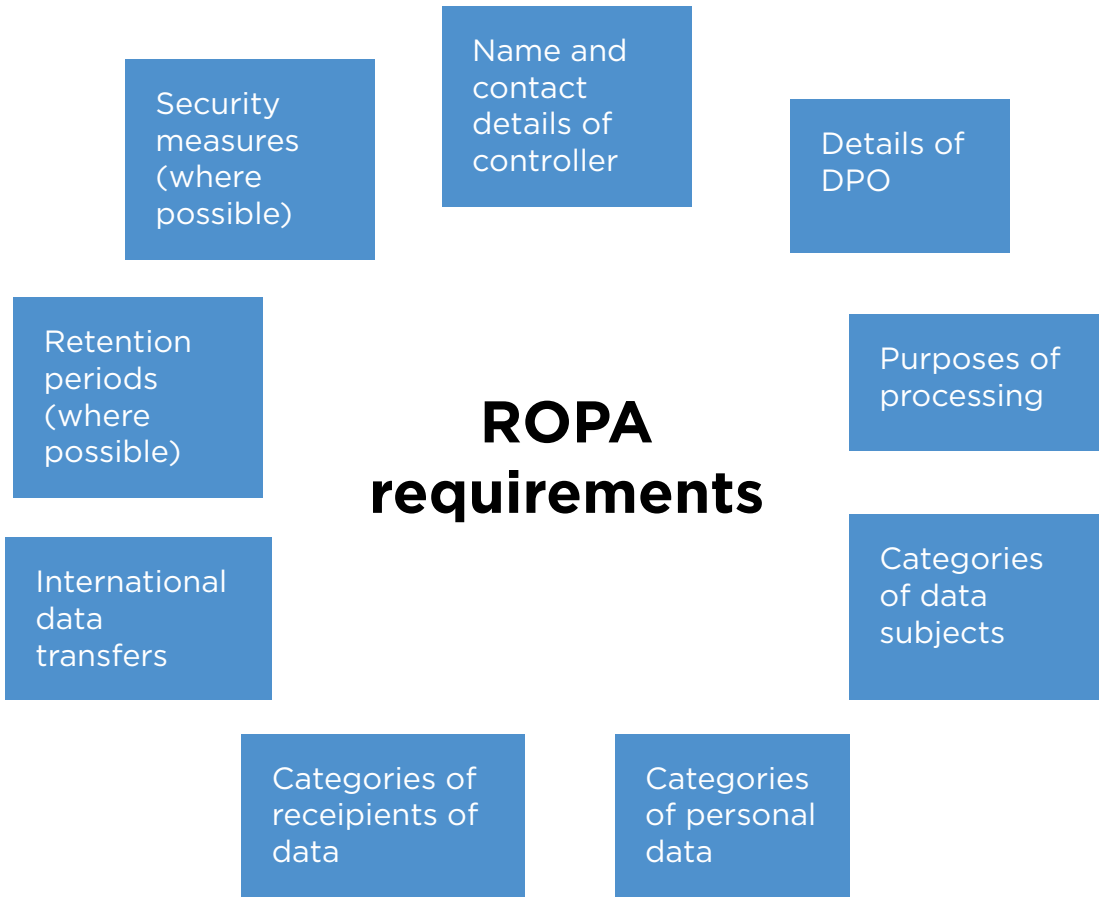
You need to put in place appropriate **'technical and organisational measures'** to meet the requirements of accountability, including:

- Adopting and implementing **data protection policies**
- Taking a **'data protection by design and default'** approach
- Putting written **contracts in place** with third parties
- **Maintaining records of your processing activities**
- Implementing appropriate **security measures**
- Recording and, where necessary, **reporting personal data breaches**
- **Carrying out DPIAs** for uses of personal data that are likely to result in high risk to individuals' interests
- **Appointing a DPO**
- **Adhering to relevant codes of conduct** and signing up to certification schemes

Accountability obligations are ongoing. You must review and, where necessary, update the measures you put in place.

Records of processing activities (ROPA)

GDPR requires that organisations with **at least 250 employees** (or less if you process special category or criminal data) must document and maintain a full overview of their processing activities.



How can you comply with this new responsibility?

- ✔ You can address it by implementing a sophisticated data mapping tool to record the necessary data by business process, or
- ✔ You can use an excel document that can be populated and maintained by the different process owners within your company (although it is more difficult to track changes this way).

Raising awareness

GDPR affects anyone who handles personal information as part of their job. Data handling and processing forms part of many roles, so GDPR **training is vital** to ensure that the GDPR requirements are met within your business. Remember, the chain is only as strong as its weakest link: everyone in your team needs to be at the top of their privacy compliance game.

- **What will you achieve by training?**

Identify the key concepts and principles of GDPR

Explore the rights of data subjects and how they apply in practice

Investigate the obligations of data controllers and processors and the steps necessary to comply with the GDPR

Understand the GDPR enforcement mechanisms

Staff and business processes change so don't forget to repeat your training periodically.

Audit

Audits play a key role in understanding and meeting your data protection obligations.

An **internal audit** is an opportunity to assess whether you have effective controls in place and whether your policies are fit for purpose. You may want to assess:

- **Data protection governance,** and the policies and procedures to ensure compliance with data protection legislation
- Processes for managing '**structured filing systems**' containing both electronic and manual records containing personal data
- **Supplier onboarding procedures and contract management**
- Processes for **responding to any request for personal data**, including requests from individuals for copies of their data as well as those made by third parties
- Technical and organisational measures in place to ensure adequate security of personal data
- Provision of staff **data protection training** and the monitoring of staff awareness

Audits can take different forms and can be carried out by private firms or the ICO and as a pre-emptive measure or where there is a suspected breach of contract or the law.

You may want to **audit your processors** to ensure that they are following your instructions and complying with applicable data protection laws. To be able to do this, you should include **audit rights in all your data processing agreements** to allow for the audit of facilities and processes of third parties who process personal data on your behalf.

Part 5 starts on the next page

Data protection toolkit

Part 5: What happens if we do something wrong?

KEMP LITTLE

ICO helpline for advice: 0303 1231113

Weblink for: online ICO reporting

Separate reporting tool for: health and care organisations

ICO online self assessment tool (to determine whether a breach must be reported)

British Airways suffered a data breach in September 2018 when 380,000 payment transactions were hacked and customer payment card details were stolen. BA began investigating as soon as the breach was discovered and they notified affected customers the following day. The CEO made press statements the next day and took out apology advertisements in national newspapers. The parent company share price instantly dropped. BA is a well-established company with a strong market share and a good safety record but this was not their first embarrassing IT issue and the airline's reputation was bound to be affected.

No matter how prepared you are, a data breach can still occur. Even if your organisation has excellent cybersecurity practices in place you can still be outsmarted by a cyberattacker or a disgruntled employee with data access or encounter human errors (see the **Morrisons case** above).

The ICO will want to see what measures your company had in place to protect the personal data of individuals and to comply with the relevant data protection laws and what steps you have taken to remedy the breach. They tend to be pragmatic (especially compared to other regulators) but you must act quickly and be able to prove that you have adequate security measures in place.

When and how to report a breach

If a **personal data breach** is **likely to affect the rights and freedoms of individuals** you must report it to the ICO (online or by telephone in an emergency in working hours) **within 72 hours** of becoming aware of the breach. Risks include identity theft, fraud, discrimination, financial loss and reputational damage.

If the breach is a likely to have a **high risk** of adversely affecting individuals' rights and freedoms you must also **inform the individuals affected without undue delay.** You will need to explain the type and volume of personal data affected, the possible consequences and the action taken. Your monitoring systems and logs should be able to assist here.

Telecom and internet service providers have to report personal data breaches to the ICO under **PECR** **within 24 hours** of becoming aware of them. Trust Service Providers must also report notifiable breaches under **eIDAS** to the ICO. Significant cyber incidents should be reported to the **NCSC** or to Action Fraud.

All entities are required to keep personal data breach logs regardless of whether those breaches have to be notified.

ICO fines

Fines have increased dramatically under GDPR. The ICO now has the power to impose fines of up to **€20M or up to 4% of a company's global annual turnover (whichever is higher) per infringement.**

The highest penalty announced so far is the ICO's notice of intention to fine **British Airways £183M** in July 2019. BA has agreed an extension of time and may be able to persuade the regulator to reduce the fine but we do expect the ICO to make an example of BA when the fine is announced (expected May 2020).

Failure to notify a breach can incur a further fine of up to €10M (or 2% of global turnover) so it is important to have an effective reporting process.

Co-operation of data protection authorities post Brexit

The ICO and EDPB have stated that they intend to keep a close working relationship between the ICO and the EU supervisory authorities now that the UK has left the EU.

Whereas EU case law, decisions and guidance will not be binding in the UK, it will undoubtedly be an ongoing point of reference. Remember that privacy is, by nature, a global subject and therefore regulators rely on each other to navigate the new issues that come up in the ever-changing privacy landscape.

Civil and criminal offences

In addition to regulatory fines, personal data breaches may attract claims for **breach of confidence, breach of copyright** and/or **database infringement**. Data subjects are also able to bring claims under the GDPR. If the breach is ongoing, the injured party may seek **injunctive relief** to prevent further data loss and later pursue a compensation **claim for damages**. Exposing the culprit or the cause of the breach may rely on information from an unwilling third party (e.g. the email/web host), which may require a **Norwich Pharmacal order** from court to extract technical details.

The **DPA 2018 criminalises:**

- Obtaining, retaining, disclosing and selling personal data without consent
- Re-identification of de-identified personal data (e.g. removing redactions/supplying the key to pseudonymised data)
- Destruction or alteration of information to prevent disclosure by a DSAR
- Obstruction of ICO inspections

These criminal offences are punishable by fines rather than custodial sentences and will only be prosecuted where it is in the public interest.

If the privacy breach is cyber related there are various **cyber dependant crimes** (e.g. **hacking/DOS attacks**) which target electronic personal data and **cyber enabled crimes** (e.g. identity fraud/data theft) which use technology (e.g. **phishing**/**malware**) to expose personal data.

Reputation management

Security incidents and personal data breaches always generate **news coverage.** However, professional and efficient handling of an incident can minimise reputational damage.

Does your organisation have an **incident management plan**, is it kept **up to date** and have you **tested** it out with your staff in a practice data breach scenario? If a member of staff left a folder of sensitive documents on the bus or discovered a data leak on social media would they know who to contact (even out of hours)? Can your IT team shut down the compromised booking or payment system and risk taking the business offline: who makes those decisions? Is there a PR strategy: how transparent should you be until you know the full story? The ICO wants you to report the breach as soon as possible but sometimes it is prudent to report the basic information first and add further details once your teams have had time to conduct a proper investigation.

If possible, the key is to reassure your customers (and potential customers) that the risk of harm is low and that it won't happen again.

Homeworking (e.g. during the Covid 19 lockdown) **increases the likelihood of security incidents**

You may want to **monitor the productivity of your employees** working from home on corporate or **BYOD** devices but you must explain this in a **privacy notice** before you start tracking them

Lessons learnt

Post – incident analysis is essential to help prevent further personal data breaches. Whether the breach was due to human error, a cyber attack, theft from unsecured premises or an unlocked filing cabinet or was just a near miss: there should be some investigation into how it occurred, the potential damage (i.e. the amount of personal data at risk and the sensitivity of that data) and how to prevent it happening again in the future.

You might discover you need to:

- Allocate more time and resources to patching software
- Use password management tools (so your staff aren't tempted to write down their passwords)
- Update your policies and procedures (e.g. is your **BYOD** policy up to scratch and are the lawful bases in your **privacy notice** up to date?)
- Conduct more staff training

It might seem like a time-consuming exercise but it may save you time, reputation and money in the long-term.

Data protection toolkit

Part 6: UK data protection law post Brexit

KEMP LITTLE

Does the GDPR still apply?

Now that the UK has a **Withdrawal Agreement** with the **EU**, there will be a **transition period until the end of 2020** to allow time to negotiate a new arrangement with the EU.

During the transition period the GDPR will continue to apply in the UK and you won't need to take any immediate action.

What happens at the end of the transition period?

That depends on negotiations during the transition period. **GDPR will no longer apply to the UK** but the provisions will be brought into UK law as the 'UK GDPR' to sit alongside the **DPA 2018, so any changes are likely to be minimal**. Watch out for further developments including how we deal with issues such as UK-EU transfers.

The GDPR may still apply if you operate in Europe, or offer goods or services into the EEA or monitor the behaviour of data subjects in the EEA.

PECR and NIS, which sit alongside GDPR as part of the family of data protection measures, will continue to apply because they are UK Regulations (derived from EU Directives).

What if my company trades in Europe but has no office there? Do we need a European representative during the transition period?

No, **during the transition period you do not need to appoint a representative in the EEA**. However, you need to check whether you offer goods or services to individuals in the EEA or monitor their behaviour as you may need to appoint a representative from the end of the transition period.

The ICO is the UK data protection regulator. During the transition period, the ICO will continue to be a lead supervisory authority (regulator with primary responsibility for cross-border processing).

Post transition the ICO will remain the independent supervisory body for data protection in the UK and will continue to work closely with other regulators worldwide and the EDPB. The ICO's pragmatic approach will likely stay the same as before Brexit.

Can we still transfer data to and from Europe?

Adequacy Decision?

The GDPR requires **adequate safeguards to be put in place for personal data transferred out of the EEA** unless the data is transferred to a **trusted country** (see the current list here), or one of the **exceptions** applies (e.g. a medical emergency or explicit consent). On July 2020 the Court of Justice of the European Union decided in the Schrems II Judgment that the "Privacy Shield" mechanism was no longer valid and, therefore, organisations can no longer rely on Privacy Shield certification to transfer personal data to the US. This Judgement may have a significant impact on data flows. For more information, please see our Key Contacts at Kemp Little.

Model clauses?

The most commonly used safeguards are **standard contractual clauses** (aka model clauses) and binding corporate rules. Based on the Schrems II Judgement, when using standard contractual clauses, a case-by-case assessment of foreign surveillance and security laws may need to be performed to determine whether these model clauses are still a valid way to transfer personal data.

BCRs?

The UK Government has confirmed that **transfers of personal data from the UK to Europe can continue from 2021 without additional safeguards.**

Exception applies?

For the time being companies can continue to transfer data from Europe to the UK as before. We will have to wait and see what is agreed for such future transfers. The UK **may have to negotiate an 'adequacy decision'** with the EDPB to prevent the need for further safeguards. Be prepared to apply additional safeguards at the request of your European partners by December 2020. You may want to start discussions with major suppliers now if you're not already using model clauses. The ICO has produced an interactive tool to help with standard contractual clauses.

Key "do's"

- Ensure that all key stakeholders are involved in the data protection requirementsJust involve the IT team
- Allocate sufficient time and resources
- Make data protection a standing item on the board meeting agenda
- Keep your incident management plan up to date and rehearse it
- Create a positive data protection culture and encourage staff to be honest if they make a mistake: it's better to know about potential problems

Key "don'ts"

- Just draft your data protection policies and procedures and put them in the filing cabinet
- Forget to carry out regular staff training sessions
- Assume that data protection doesn't matter – IT DOES!
- Underestimate the size of the task involved in implementing data protection compliance
- Neglect to update your data processing records

How Kemp Little can help you...

Running data protection awareness and education briefings/training

Checking service contracts and sub-contracts

Drafting data protection policies and procedures

Providing KLick DPO support

Advising on/providing legal privilege

Assisting with data protection audits

Advising on remediation

Advising on data breaches

Please see our cyber security toolkit for more information on cybersecurity

Glossary begins on the next page

Data Protection toolkit

Glossary

KEMP LITTLE

B-C

Binding corporate rules

- BCRs are an internal code of conduct operating within a multinational group, which apply to restricted transfers of personal data from the group's EEA entities to non-EEA group entities.

BYOD (Bring Your Own Device) policy

- A policy which mitigates the security risk of allowing employees to use their personal laptops, tablets and smartphones to connect to corporate networks.

Cookies

- Cookies are small pieces of information (normally just letters and numbers) stored by software on the user's device (e.g. a web browser) used by the owner of a website to identify or track users. There are many types of cookies including 'session' or 'persistent' cookies (depending on how long they are stored for) and 'first-party' or 'third-party' cookies (depending on who sets them).

D

Data flow map

- Deliberate actions to alter, disrupt, deceive, degrade, or destroy information systems/information networks or the information and/or programs within them.

Data subject

- Any human being.

Data protection by design and default

- The requirement to implement appropriate technical and organisational measures to implement the **data protection principles** and implement necessary processing safeguards as required by Article 25 of the GDPR.

Direct marketing

- The communication (by whatever means) of advertising or marketing material which is directed to particular individuals as defined in section 122(5) of the Data Protection Act 2018.

DOS (denial of service) attack

- Creating a denial of service by flooding the bandwidth or resources of (or otherwise crashing) a targeted information system using a single unique IP address; preventing legitimate users of a service from accessing that service.

E

EDPB

- The European Data Protection Board is an independent European body, which contributes to the consistent application of data protection rules throughout the EU and promotes cooperation between the EU's data protection authorities.

EEA

- The European Economic Area includes EU countries plus Iceland, Liechtenstein and Norway. It allows them to be part of the EU's single market. Switzerland is not an EU or EEA member but is part of the single market. This means Swiss nationals have the same rights to live and work in the UK as other EEA nationals.

eIDAS

- Sets out rules for electronic identification (individuals and documents) and trust services for electronic transactions. The ICO is the supervisory body for UK trust service providers. The UK eIDAS Regulations were amended by the **Data Protection Act 2018.**

GDPR

G-L

- Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation).

ICO (Information Commissioner's Office)

- A non-departmental public body charged with policing and enforcing the data protection regime in the UK.

Lawful basis

- Personal data may only be processed if one of the following lawful bases in Article 6 of the GDPR applies:
  - Consent
  - Necessary for contractual performance
  - Compliance with a legal obligation
  - Protection of the vital interests of a data subject
  - Public interest
  - Legitimate interest
- Special category personal data may only be processed if one of the lawful bases in Article 9 of the GDPR applies.
- Criminal conviction data may only be processed if one of the conditions set out in Schedule 1 of the DPA 2018 is met.

M-N

Malware

- Software or firmware intended to perform an unauthorised process that will have an adverse impact on the confidentiality, integrity, or availability of an IT system, including viruses, worms, trojan horses and spyware.

Multi-factor authentication and two step authentication

- A method of controlling computer access by requiring a user to successfully complete several separate authentication stages using credentials based on knowledge or possession.

NCSC (National Cyber Security Centre)

- The UK Government's technology authority, set up to provide guidance and advice on cybersecurity for UK organisations.

NIS

- The Network Information Security Regulations 2018 concern the security of systems and apply to 'operators of essential services' (OES) and 'relevant digital service providers' (RDSPs).

Norwich Pharmacal order (aka third party disclosure order)

- An equitable form of relief granted which requires a respondent to disclose certain documents or information to an applicant. Typically, the applicant knows that wrongdoing has occurred but cannot identify the wrongdoer, only a third party with relevant information.

P-S

PECR

- The Privacy and Electronic Communications Regulations give people specific privacy rights in relation to electronic communications and restrict unsolicited marketing by phone, fax, email, text, or other electronic message. They also restrict accessing and storing material on a user's device (i.e. cookies/similar technologies). The EU is developing a new e-privacy Regulation but it has not yet been agreed.

Phishing

- Tricking individuals into disclosing information through deceptive IT-based means.

Privacy notice

- A method of informing individuals about the collection and use of their personal data in accordance with Articles 12-14 of the GDPR.

Profiling

- The compilation of profiles for the purpose of categorising people, based on which predictions can be made on behaviour and interests. This may be done for direct marketing purposes (such as the provision of newsletters and offers), but also for generating automated decisions.

Spear-fishing

- A variation of **phishing** where the email sent to the targeted individual is personalised so as to appear to be from an individual or business with whom the target is familiar.

Special category data

- Personal information of data subjects that is especially sensitive, the exposure of which could significantly impact the rights and freedoms of data subjects. GDPR special category data includes:
    - Race and ethnic origin
    - Religious or philosophical beliefs
    - Political opinions
    - Trade union memberships
    - Biometric data used to identify an individual
    - Genetic data
    - Health data
    - Data related to sexual preferences, sex life, and/or sexual orientation

Standard contractual clauses

- Standard clauses approved by the Commission to be entered into by the data exporter (based in the EEA) and the data importer (outside the EEA) containing contractual obligations which protect the rights for the individuals whose personal data is transferred. There are separate clauses for controller to controller and controller to processor transfers. Note that the Commission plans to update the existing clauses.

Data Protection toolkit

Other useful resources

KEMP LITTLE

ICO

Guide to the General Data Protection Regulation

https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf

Guide to Direct Marketing

https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf

Guidance on post Brexit compliance

https://ico.org.uk/for-organisations/data-protection-and-brexit/

Guidance on the use of cookies and similar technologies

https://ico.org.uk/media/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies-1-0.pdf

European Data Protection Board

Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - version adopted after public consultation

https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en

Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 - version adopted after public consultation

https://edpb.europa.eu/our-work-tools/our-documents/wytyczne/guidelines-12019-codes-conduct-and-monitoring-bodies-under_en

Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects

https://edpb.europa.eu/our-work-tools/public-consultations/2019/guidelines-22019-processing-personal-data-under-article-61b_en

Recommendation 01/2019 on the draft list of the European Data Protection Supervisor regarding the processing operations subject to the requirement of a data protection impact assessment (Article 39.4 of Regulation (EU) 2018/1725)

https://edpb.europa.eu/our-work-tools/our-documents/zalecenia/recommendation-012019-draft-list-european-data-protection_en

Guidelines 3/2019 on processing of personal data through video devices - version adopted after public consultation

https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en

Guidelines 4/2019 on Article 25 Data Protection by Design and by Default

https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en

Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR

https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-52019-criteria-right-be-forgotten-search_en

European Commission model clauses

Controller to controller (decision 2004/915/EC)
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004D0915&from=EN
Controller to processor
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010D0087&from=en

NCSC

5 questions for your board's agenda
https://www.ncsc.gov.uk/guidance/board-toolkit-five-questions-your-boards-agenda

> **The key difference Kemp Little brings to the table is a firmly pragmatic and solution-focused view and a young vibrant outlook.**

Client quote
The Legal 500
Client's Guide to the Best Law Firms

Your key contacts

Anita Bapat
Partner
Data Protection & Privacy
ddi +44 (0) 20 7710 8033
anita.bapat@kemplittle.com

Alex Dittel
Senior Associate
Data Protection & Privacy
ddi +44 (0) 20 7710 1648
alex.dittel@kemplittle.com

Marta Dunphy-Moriel
Partner
Data Protection & Privacy
ddi +44 (0) 20 7710 1618
marta.dunphy-moriel@kemplittle.com

Aneka Chapaneri
Associate
Commercial Technology
ddi +44 (0) 20 7710 1631
aneka.chapaneri@kemplittle.com

Emma Wright
Partner
Commercial Technology
ddi +44 (0) 20 7710 8003
emma.wright@kemplittle.com

Agatha Claridge
Associate
Data Protection & Privacy
ddi +44 (0) 20 7710 8043
agatha.claridge@kemplittle.com

Nicola Wise
Consultant
Data Protection & Privacy
ddi +44 (0) 20 7710 8022
nicola.wise@kemplittle.com

Judit Garrido-Fontova
Associate
Data Protection & Privacy
ddi +44 (0) 20 7710 1618
judit.garrido-fontova@kemplittle.com

Matthew Gregson
Associate
Data Protection & Privacy
ddi +44 (0) 20 7710 1638
matthew.gregson@kemplittle.com

www.kemplittle.com
https://www.kemplittle.com/services/data-protection-privacy/

KEMP
LITTLE