White&Black

Reflections on GDPR One Year On

London & Oxford | Technology | Corporate | Disputes

Who we are

- Corporate & Technology Lawyers
- Founded in 2007
- Locations in Oxfordshire and London
- Areas of practice (Chamber & Partners 2019 rankings):
  - Private equity: venture capital and investment
  - Corporate/ M&A (mid-market & private equity)
  - Intellectual Property
  - Data Protection
  - Information Technology
  - Litigation
- The Times – Best Law Firms 2019

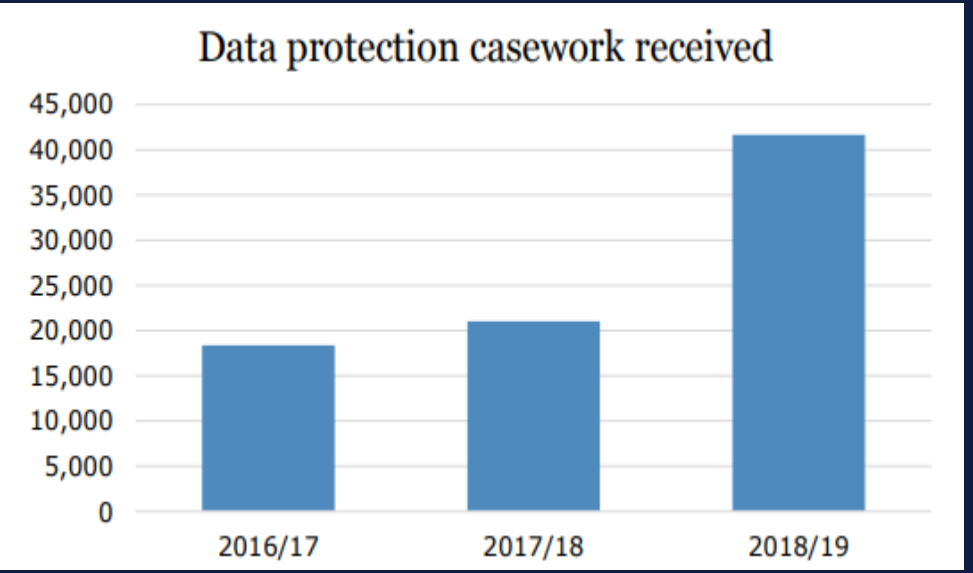
- Victoria Wright: Victoria.Wright@wablegal.com
- Nick Mitchell: Nicholas.Mitchell@wablegal.com

Regulatory Recap

Regulatory Recap

What has changed since 25 May 2018?

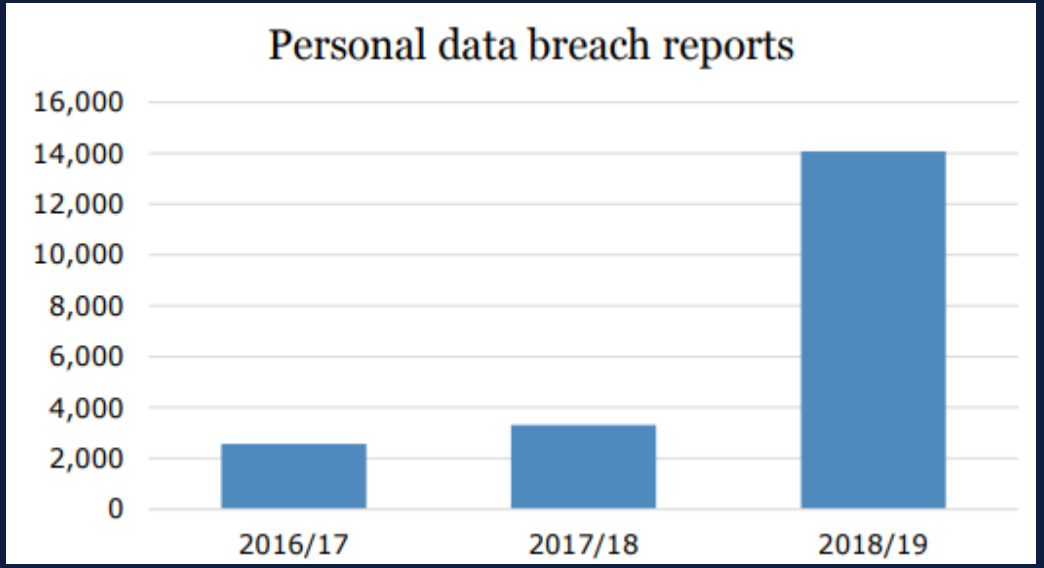
- There has been a significant increase in the public's awareness of their data rights and a willingness to enforce those rights.
- 40,000 data protection complaints have been reported to the ICO.
- 38% of these complaints related to subject access requests.
- Health sector, local government and lenders have seen the highest number of complaints.



Regulatory Recap

- Businesses are also taking their new obligations seriously and are proactively and systemically engaging with the appropriate authorities.

- 14,000 personal data breaches reported to the ICO – an average of 41 per day.
  - 17.5% required action from the organisation involved.
  - 0.5% led to an improvement plan or civil monetary penalty – however the vast majority of enforcement actions are still being brought under the old law.



Regulatory Recap

What about enforcement?

It is still early days for GDPR enforcement. The ICO have yet to issue a fine under the GDPR, however three fines have been issued in Europe:

- Germany imposed a €20,000 fine on a social network operator for failing to protect users' personal data.
- Austria imposed a €5,280 fine on a sport betting café for unlawful video surveillance.
- France imposed a €50 million fine on Google for alleged lack of consent to personalised ads.

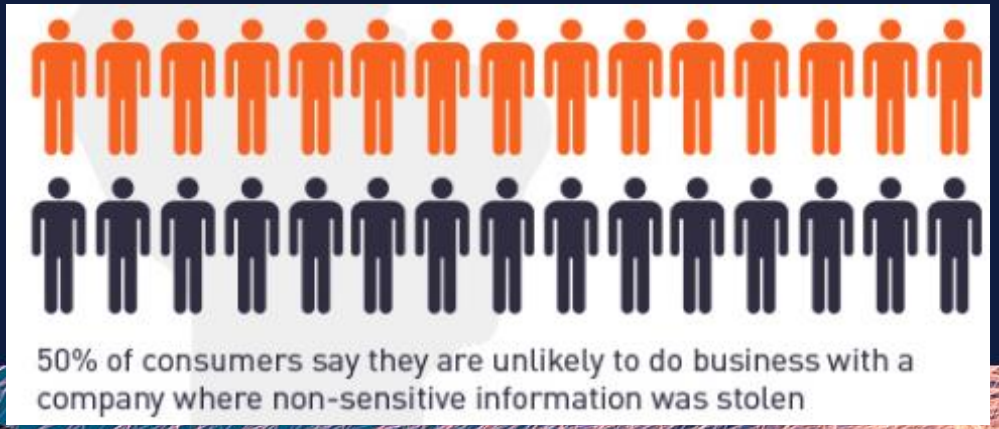
- We expect to see more fines issued this year as regulators work through their backlog.

Regulatory Recap

Are there other benefits to compliance?

- 61% or organisations have reported that by undertaking compliance activities – such as improving record processing or taking a detailed analysis of their internal systems – has yielded benefits other than just merely being on the right side of the law.

- 21% of organisations expect to see 'significant benefits' including competitive advantage, improved reputation, business enablement and better engagement with consumers as a result of increased transparency.



Data Protection and Employment

Data Protection Principles

The GDPR sets out 7 principles which data controllers and processors must comply with when processing personal data. These are core obligations and must be considered at all stages of employment – from recruitment through to exit.

The data controller must process personal data in accordance with the principles (Art 5 GDPR)

Lawfulness, fairness and transparency:	PD must be processed lawfully, fairly and in a transparent manner in relation to the data subject
Purpose limitation:	PD must only be collected for specified, explicit and lawful purposes and only processed in a compatible way
Data minimization:	PD must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
Accuracy:	PD must be accurate and, where necessary, kept up to date
Storage limitation:	PD must be kept in a form which permits identification of data subjects for no longer than is necessary for purposes for which PD was collected
Integrity and confidentiality:	PD must be processed in a way that ensures appropriate security – "appropriate technical and organisational measures
Accountability:	The controller shall be **responsible** for, and be able to **demonstrate compliance** with the data protection principles." GDPR Art. 5(2)

Recruitment

Recruitment

Recruitment best practice involves documenting the key stages of the process and evidencing the decisions taken by the employer. The GDPR does not change this.

The GDPR requires that the employer consider more carefully how it handles the data of the applicant in line with the Data Protection Principles.

Some key points to consider are:

- How does the employer deal with the personal data it receives from job applicants?
- How does the employer conduct equal opportunities monitoring as part of a recruitment exercise?
- What does the employer do with the information it has received at the end of a recruitment exercise?

Recruitment

Lawfulness, fairness and transparency:	Applicants should be made aware of how the employer will process their personal data and for how long. A candidate privacy notice, for example via a statement in the job advertisement, should be supplied setting this out.
Purpose limitation:	Applicant data should be used for recruitment purposes only. The employer must not use this data for anything outside of this purpose.
Data minimization:	The employer should carefully consider what data it requires from the applicant in order to complete the recruitment process. Requests for unnecessary data should be avoided.
Accuracy:	Addresses, phone numbers etc. should be kept up to date.
Storage limitation:	How long will the personal data be retained for? Until the end of the recruitment cycle or longer? Why?
Integrity and confidentiality:	The employer must ensure it has systems in place, whether physical or digital, to ensure the personal data of the applicant remains confidential and secure.
Accountability:	The employer must be able to demonstrate its rationale for the handling of the applicant data.

Recruitment

Automated Decision Making

Automated decision making is the process of making a decision by automated means without any human involvement.

These decisions can be based on factual data, as well as on digitally created profiles or inferred data, e.g. an aptitude test used for recruitment which uses pre-programmed algorithms and criteria.

The GDPR limits the circumstances in which you can make solely automated decisions that have a **legal** or **similarly significant effect on individuals.**

A process won't be considered solely automated if someone weighs up and interprets the result of an automated decision before applying it to the individual.

Token human involvement, such as merely applying the decision taken by the automated system, is not acceptable.

Onboarding

Onboarding

The Employment Contract & the Problem With Consent

- Employment contracts before GDPR were often drafted on the basis of employee consent to processing.
- Myth that consent is a “silver bullet” for GDPR compliance
- Art 4 GDPR states that consent must now be “freely given” and can be withdrawn at any time.
- The ICO and Art29WP/EDPB have stated that due to the imbalance of power in the employment relationship, consent cannot and should not be used as the basis for the majority of data processing at work.

Onboarding

The Employment Contract & the Problem With Consent

Employers must rely upon an alternative basis for the processing of employee personal data such as:

- necessity for the performance of a contract;
- compliance with a legal obligation; or
- employer's legitimate interests (conduct an assessment).

Onboarding

- With a successful applicant selected and an appropriate basis for processing identified, the employer will now need to decide what information should be transferred to the employee's personnel file.
- This should be limited to information relevant to the ongoing employment relationship.
- Employees must be made aware of what data is being processed about them and the retention periods.

New Starter Form

Private Details

Full Name:		Title:	
Home Address:		Home Tel No:	
		Mobile No:	
		Date of Birth:	
<Town>	<Post Code>	Marital Status:	
E-Mail address:		NI No:	
Trade Union Membership No:			

Job Details

Start Date:		Probation Period:	
Department:		Line Manager:	
Position:		Term:	
Salary:		Status:	

Bank Details

Bank Name:		Branch Name:	
Branch Address:		Account No:	
		Sort Code:	
<Town>	<Post Code>		

Next of Kin Details

Full Name:		Relationship:	
Address:		Home Tel No:	
		Work Tel No:	
<Town>	<Post Code>	E-mail Address:	

Do you have any health issues we should know about? Please provide details.

Equality & Diversity

Gender:	
Religion:	
Sexual Orientation:	

New Starter Form

Private Details

Full Name:		Title:	
Home Address:		Home Tel No:	
		Mobile No:	
		Date of Birth:	
<Town>	<Post Code>	Marital Status:	
E-Mail address:		NI No:	
Trade Union Membership No:			

Job Details

Start Date:		Probation Period:	
Department:		Line Manager:	
Position:		Term:	
Salary:		Status:	

Bank Details

Bank Name:		Branch Name:	
Branch Address:		Account No:	
		Sort Code:	
<Town>	<Post Code>		

Next of Kin Details

Full Name:		Relationship:	
Address:		Home Tel No:	
		Work Tel No:	
<Town>	<Post Code>	E-mail Address:	

Do you have any health issues we should know about? Please provide details.

Equality & Diversity

Gender:	
Religion:	
Sexual Orientation:	

Onboarding

Special Categories of Personal Data

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic and biometric data (for the purpose of uniquely identifying a person).
- Health
- Sex life or sexual orientation

Processing special categories of personal data is prohibited unless an exception applies, e.g.:

- Explicit Consent
- Necessary for the performance of rights and obligations in connection with employment
- Legal Claims
- Health Purposes

Onboarding

In connection with employment obligations

- The processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the employer or employee in connection with employment.

- When the processing is carried out, the employer has an appropriate policy in place.

- The employer must put in place additional safeguards such as ensuring that the relevant policy documents are kept up-to-date and a record documenting processing activities exists.

Onboarding

Explicit Consent

- Consent must be: specific, informed and unambiguous indication of the individual's wishes. ”Explicit" consent must also be affirmed in a clear statement – either written or oral.

- Same problems as with ordinary consent.

- There may be limited circumstances where explicit consent is appropriate because if it were withdrawn, it would not interfere with the general management of staff – e.g. sensitive health data.

Onboarding

Health Data

Processing of this data is permitted where it Is necessary:

- For the purposes of preventive or occupational medicine.
- For the assessment of the working capacity of the employee.
- For the purposes of medical diagnosis.
- For the provision of health or social care or treatment or the management of health or social care systems and services.

Legal Claims

- Where processing is necessary for the establishment, exercise or defence of legal claims, or whenever courts are acting in their judicial capacity.

Onboarding

Criminal Conviction Data

- Now a separate category of data to special category data.
- Article 10 GDPR, Articles 9 and 10 and Schedule 1 to DPA 2018.
- Similar to special category processing, the employer should have an appropriate policy and safeguards in place.

Onboarding

<u>Criminal Conviction Data: Lawful bases</u>

Grounds for processing criminal conviction data include:

- Necessary in connection with employment where obligations/rights are imposed or conferred by law (Part 1, Sch 1, DPA 2018)

- Necessary for Substantial Public Interest conditions (Part 2, Sch 1)
  - Includes regulatory requirements relating to unlawful acts, dishonesty etc

- Other grounds (Part 3, Sch 1):
  - If the employee consents (unlikely to be valid)
  - Necessary to protect vital interests of an individual
  - Specific carve-out for legitimate activities of not-for-profits
  - Personal data that has manifestly been made public by the employee
  - Necessary in connection with legal claims, obtaining legal advice etc

Employment

Employee Data

Demonstrating compliance

- Data protection by design and default – evidence compliance with the data protection principles in all aspects of processing and data handling
- Only process personal data necessary for an intended, specific purpose
- Consider what employee monitoring occurs and legal basis
- Technical and organisational measures (system security, device security)
- Keep records of processing activities and perform assessments
- Data protection policies and regular training
- Minimum processor terms for suppliers who process data (e.g. payroll)

Employee Data

Data subject rights

- Right of access
- Right to rectification
- Right to erasure
- Right to restriction of processing
- Right to data portability
- Right to object

Employee Data

Data Subject Access Requests

An employee has the right to obtain from an employer information as to whether or not personal data is being processed about him or her.

If personal data is being processed, the employee is entitled to be given a copy of his or her personal data together with the following information:

- the purposes of the processing
- the categories of personal data concerned;
- the recipients or categories of recipients to whom data has been or will be disclosed
- the period during which personal data will be retained
- information on the source of the data
- information regarding complaints and disputes: the right to complain to a supervisory authority, the right to request rectification or erasure of personal data, to object to processing of data or to restrict that processing
- where personal data is transferred outside the EEA, information on any Article 46 safeguards (for example, use of model clauses or binding corporate rules)

Employee Data

Data Subject Access Requests

Responding to a subject access request can be time-consuming and expensive. However it is imperative that employers take all requests seriously.

- The employer must facilitate the exercise of the subject access right and must be willing to explain how it handled the request e.g. the steps taken to locate the data.
- The request must be handled fairly and transparently
- Information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language
- No fee chargeable unless the request is manifestly unfounded or excessive

Employee Data

How to Respond to Data Subject Access Requests

Initial assessment

- Is the employee's data actually processed?
- The scope of the request and how to go about retrieving relevant data.
- Do you intend to respond - manifestly unfounded or excessive?
- Understanding what the employee wants.

Checking identity of person making request

Timing

- 'Without undue delay' and in any case within 1 month of the receipt of request.
- If the response period needs to be extended the employer should make the employee aware within the first month.

Consider other data subjects' rights in the information provided

Employee Data

Data Breaches

- New mandatory notification requirement to ICO where a risk to rights and freedoms (72 hours)
- Mandatory notification to employees where a high risk to rights and freedoms (without undue delay)
- Technical measures can prevent an incident being a personal data breach or reduce risk profile (e.g. encryption)
- ICO enforcement including fines
- Civil actions for distress (including where the employer is compliant but the breach is by a criminal insider)

Exit

Departing Employees

- Retention periods – consider employment claims, limitation dates
- Deletion of employee data – personal emails?
- Ensuring employees do not take personal data with them (recruitment consultant prosecutions and fines)
- Tactical use of subject access requests in employment law disputes – but note that this is no defence to non-compliance with the request

Questions?

“A cutting-edge, commercially savvy and client-focused firm”

Chambers

W&B
wablegal.com

“White & Black’s overall level of service is nothing short of outstanding”

Legal 500

Oxford Office Home Park | Grove Road | Bladon | OX20 1FX
London Office 94 Jermyn Street | St James’s | SW1Y 6LE