FENWICK ELLIOTT

The construction & energy law specialists

GDPR and the Arbitrator/Adjudicator

Presentation by Simon Tolson of Fenwick Elliott LLP

FENWICK ELLIOTT

Why am I here with an arm up my back? Mmmmm…

The EU *General Data Protection Regulation* (GDPR) is the most important change in data privacy regulation in over 20 years.

The EU General Data Protection Regulation (GDPR) replaced the Data Protection Directive 95/46/EC.

The Data Protection Act 2018 replaced the DPA 98.

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

You need this puppy too: https://gdpr-info.eu/

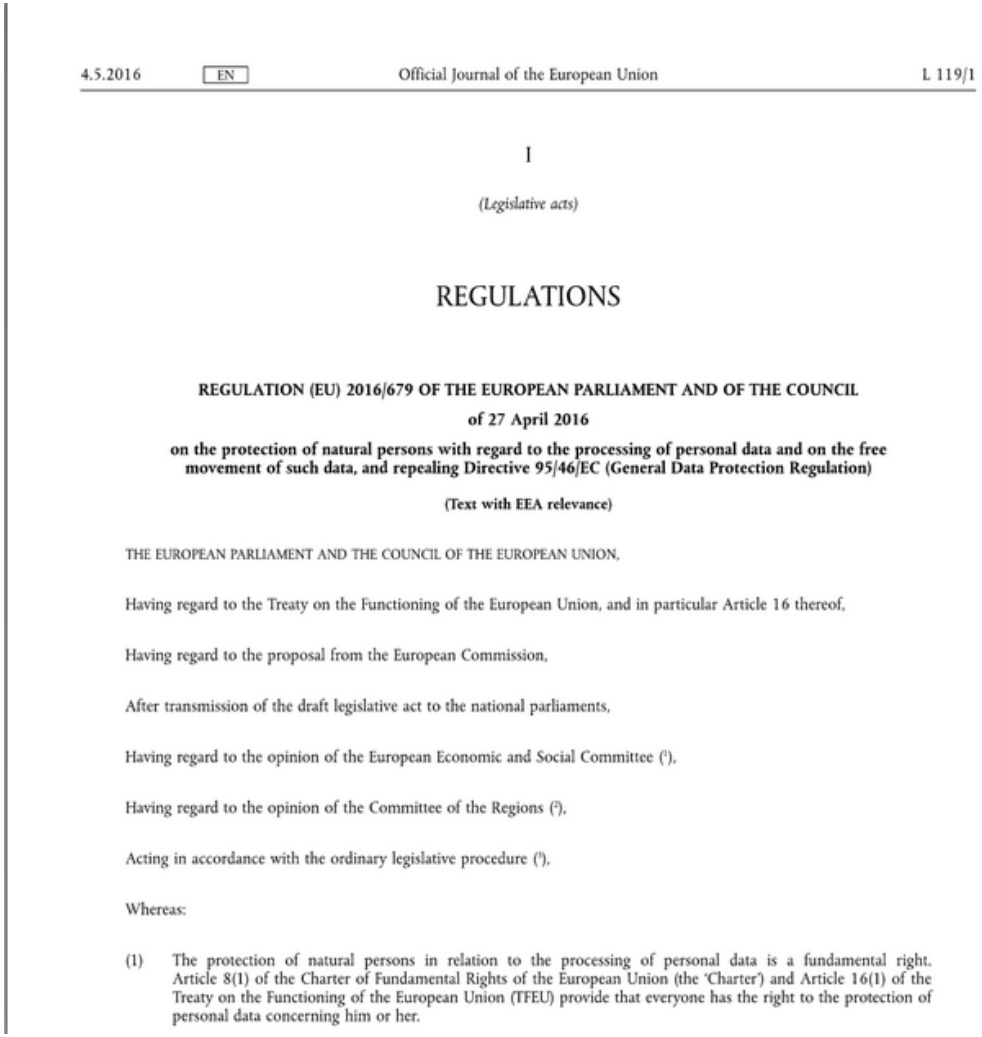
What has GDPR to do with arbitrators and adjudicators?

Bear with me on this wee journey…

The construction & energy law specialists

https://publications.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-en

FENWICK ELLIOTT



I

(Legislative acts)

REGULATIONS

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 27 April 2016

on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee ([1]),

Having regard to the opinion of the Committee of the Regions ([2]),

Acting in accordance with the ordinary legislative procedure ([3]),

Whereas:

(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

The construction & energy law specialists

GDPR (EU) 2016/679

FENWICK ELLIOTT

GDPR is the most important data privacy law thus far

Convoluted product of a four-year deliberative process

A "staggeringly complex" law that "no one really understands,"

An 88-page monster translated into 26 different languages.

GDPR is 99 Articles, 11 Chapters, 56,000 words which is about the length of William Faulkner's *As I Lay Dying.*

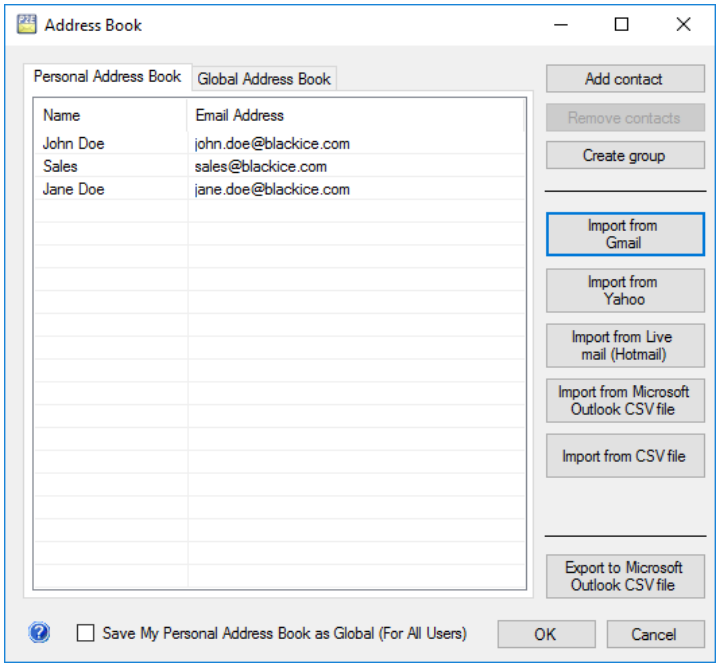
The construction & energy law specialists

Some of us can ignore GDPR

FENWICK ELLIOTT

- You will not be subject to the GDPR if you keep personal contacts', the vet, your best man and that sort of information on your computer, think in the course of personal or household activity.

- Ditto if you have CCTV cameras on your house to deter crooks. This means you wouldn't be subject to the Regulation per se.



Non-electronic documents which are not filed, (i.e. it's data you can't search for), e.g. a random piece of microfiche, or a paper notepad, are not classed as personal data in the GDPR and are therefore not subject to the right to erasure.

The construction & energy law specialists

Emergency contact details

FENWICK ELLIOTT

It is fine for an organisation to keep emergency contact details. The GDPR allows organisations to process next of kin details, including in-death-beneficiary and emergency contact details under legitimate interest processing rules or lawful bases.

Aka 'legitimate interest processing'.

Personal data must be adequate, relevant and limited to information which is necessary in relation to the purposes for which it is processed.

Personal data must be kept in a form which obviously permits identification of data subjects for no longer than necessary for the purpose for which the data is processed.

Personal data may be stored for longer periods if the personal data is processed solely for archiving purposes in the public interest or scientific and historical research processes or statistical purposes.

At this stage some suggest GDPR is less significant to daily life

FENWICK ELLIOTT

The construction & energy law specialists

For most of us we must pay some homage to it

FENWICK ELLIOTT

If you are in business then take caution.

ICO v Noble Design and Build (2018)

Noble Design and Build of Telford, Shropshire, which operates CCTV systems in buildings across Sheffield, broke data protection laws by failing to comply with an Information Notice. It was fined £4,500 for processing personal data without registering with the UK's data protection watchdog.

This law is meant to be good for you…

The construction & energy law specialists

Various Claimants v Wm Morrisons Supermarket PLC

FENWICK ELLIOTT

What about compensation claims?

The GDPR sets out a right for individuals to seek compensation for either material or non-material loss which they suffer as a result of infringements by either controllers or processors.

This is not a new concept. It was possible for individuals to raise claims under the Data Protection Act 1998. A recent example in December 2017 was the case of *Various Claimants v Wm Morrisons Supermarket PLC* [2017] EWHC 3113 where 5,518 employees claimed compensation from Morrisons on the basis of the actions of an employee who has posted personal data of around 100,000 of Morrisons employees on the internet. (He got 8 yrs. in the pokey).

Whilst it is difficult for individuals to claim a large amount of compensation for a personal data breach, group actions where a breach has affected a large number of individuals such as the *Morrisons* case may prove very costly.

Long arm of the law

FENWICK ELLIOTT

Privacy cases have always attracted significant damages for distress. The leading case of *Gulati & Ors v MGN Limited* received a great deal of publicity. In that case the court awarded various celebrities, who were victims of phone hacking, between £72,500 and £260,250 as compensation for the distress they had suffered.

Since the landmark case of *Google Inc v Vidal-Hall and others* [2015] compensation *may now be awarded for distress without the need to first prove financial loss*. Right to compensation for distress is now enshrined in the GDPR.

This *Vidal-Hall* decision unlocked the potential for successful claims for distress. Awards of between £2,500 and £12,500 were awarded to six asylum seekers when their personal data was inadvertently published on the Home office website (*TLT v Secretary of State for the Home Department* [2016]).

When making an award the court will look at the specific circumstances of the case and take into account various factors, such as the sensitivity of the data disclosed and the nature of the disclosure.

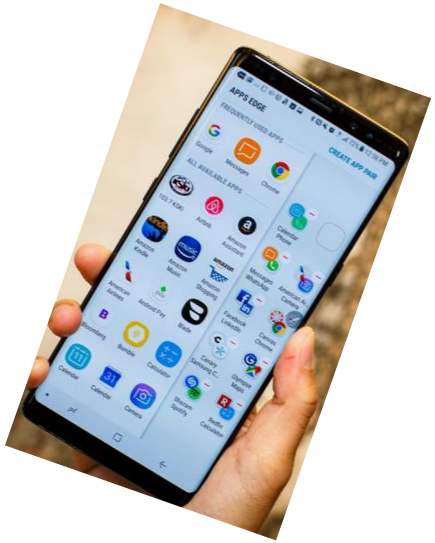
This GDPR law is meant to be good for you…

FENWICK ELLIOTT

The way apps undermine user privacy with sneaky tricks like bundling requests together, hiding the most privacy-friendly settings or using questionable advertising permissions.

Take the pop-up on the AccuWeather app – which said it shared data with 199 partners – that appeared when the testers were trying to read the list of third-party advertisers (there are 18 unaffiliated providers of advertising it shared the data with). The app then suggested the user paid a charge to avoid targeted advertising.

Another bugbear was location tracking - as well as noting Google's already well documented and much criticised not-really-off tracking activities, Which? also raised questions about Amazon's shopping app.



The construction & energy law specialists

Data security

FENWICK ELLIOTT

Data security - a red-hot topic at the moment.

The gaudy details of the **Cambridge Analytica/Facebook debacle** involved the collection of personally identifiable information of 87 million Facebook users that Cambridge Analytica used for political purposes.

A watershed moment - public understanding of personal data - precipitated a massive fall in Facebook's stock price - calls for tighter regulation of tech companies' use of data.

AND… just 21 days ago **Facebook** hackers stole digital login codes so they could take over another 50 million user accounts in its **worst security breach ever - unprecedented level of access** …a difficult year for **Facebook's** reputation and boy the class actions US and UK !

Facebook disclosed just before the 72-hour window for disclosing the news to privacy commissioners. The Hacker is the well known Taiwanese = *Chang Chi-yuang*

ICO Deputy Commissioner of operations, James Dipple-Johnstone, said:

> "It's always the company's responsibility to identify when UK citizens have been affected as part of a data breach and take steps to reduce any harm to consumers.
> "We will be making enquiries with Facebook and our overseas counterparts to establish the scale of the breach and if any UK citizens have been affected."

The construction & energy law specialists

Facebook…

FENWICK ELLIOTT

Hours after Facebook 50 million users were "directly affected" by the data breach, two of the social network's users had come together in a **class-action lawsuit**.

Facebook alerted users that a security issue had been discovered on Tuesday, 25 Sept. A vulnerability in the site's "View As" feature — which lets users see what others do when viewing their profile - gave hackers the means to take over people's accounts.

It's a bad situation that subsequently grew worse. It became clear that Facebook users who had connected their profile to an Instagram account — and, potentially, any other third-party service — were at risk on those other platforms as well.

Now there's this lawsuit, which names Carla Echavarria of California and Derrick Walker of Virginia as plaintiffs. The document also notes that the filing is "on behalf of all persons in the United States ... whose PII was compromised in the data breach."

Facebook…

FENWICK ELLIOTT

ICO the max of £500,000

In the first quarter of 2018, Facebook took £500,000 in revenue every five and a half minutes. Because of the timing of the breaches, the ICO unable to levy the penalties introduced by the European General Data Protection (GDPR), which caps fines at the higher level of €20m (£17m) or 4% of global turnover preceding financial year, whichever is the greater – in Facebook's case, $1.9bn (£1.4bn). The £500,000 cap was set by the Data Protection Act 1998.

The construction & energy law specialists

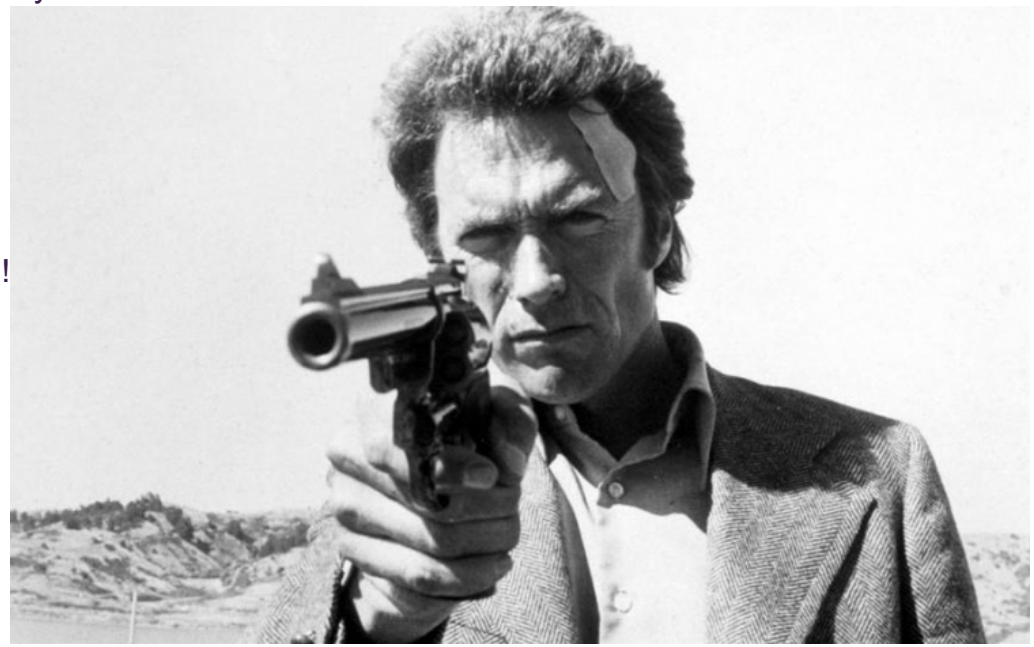
Suffering from GDPR fatigue

FENWICK ELLIOTT

The real pain in the backside … since **25 May 2018** for many construction professionals, …adjudicators and arbitrators, lawyers – and businesses is the focus on the (less electrifying provisions) of the ***General Data Protection Regulation (GDPR)***, EU law together with its sweetheart the **Data Protection Act 2018** came into force two days earlier on **23 May**.

Some thoughts are…best shared pictorially. . .

Say GDPR…Just one more time buddy!!



The construction & energy law specialists

The pain in the backside that comes with GDPR

FENWICK ELLIOTT

Note:

Fees: Organisations will no longer be able to charge the previous £10 fee, which (though minimal) did act as a limited deterrent.

Unfounded or excessive requests: Where a DSAR is "manifestly unfounded or excessive", the organisation can refuse to respond. The burden is on the organisation to show that the DSAR was manifestly unfounded or excessive in character.

Time limit for response: An organisation must respond to a DSAR without undue delay and, in any event, within one month of receipt. This is shorter than the current 40-day period that UK organisations have been used to. The one-month period can be extended to three months, taking into account the complexity and number of DSARs, in which case the data subject must be informed of the extension (including reasons) within one month of receipt of the DSAR.

Content of response: As well as access to the data subject's personal data, *the right of access extends to other information, including: the envisaged storage period for the personal data;* the right to request rectification, erasure or restriction of processing; the right to lodge a complaint with the Data Protection Authority; and, if automated decision-making is used, meaningful information on the logic involved.

What a load of bumf we all got!

FENWICK ELLIOTT

Much has been printed about the GDPR and its potential consequences (and costs) for companies and individuals.

The extensive duties placed on data controllers and processors, and the potential for significant penalties. There are two tiers of administrative fines that can be levied as penalties for non-compliance:

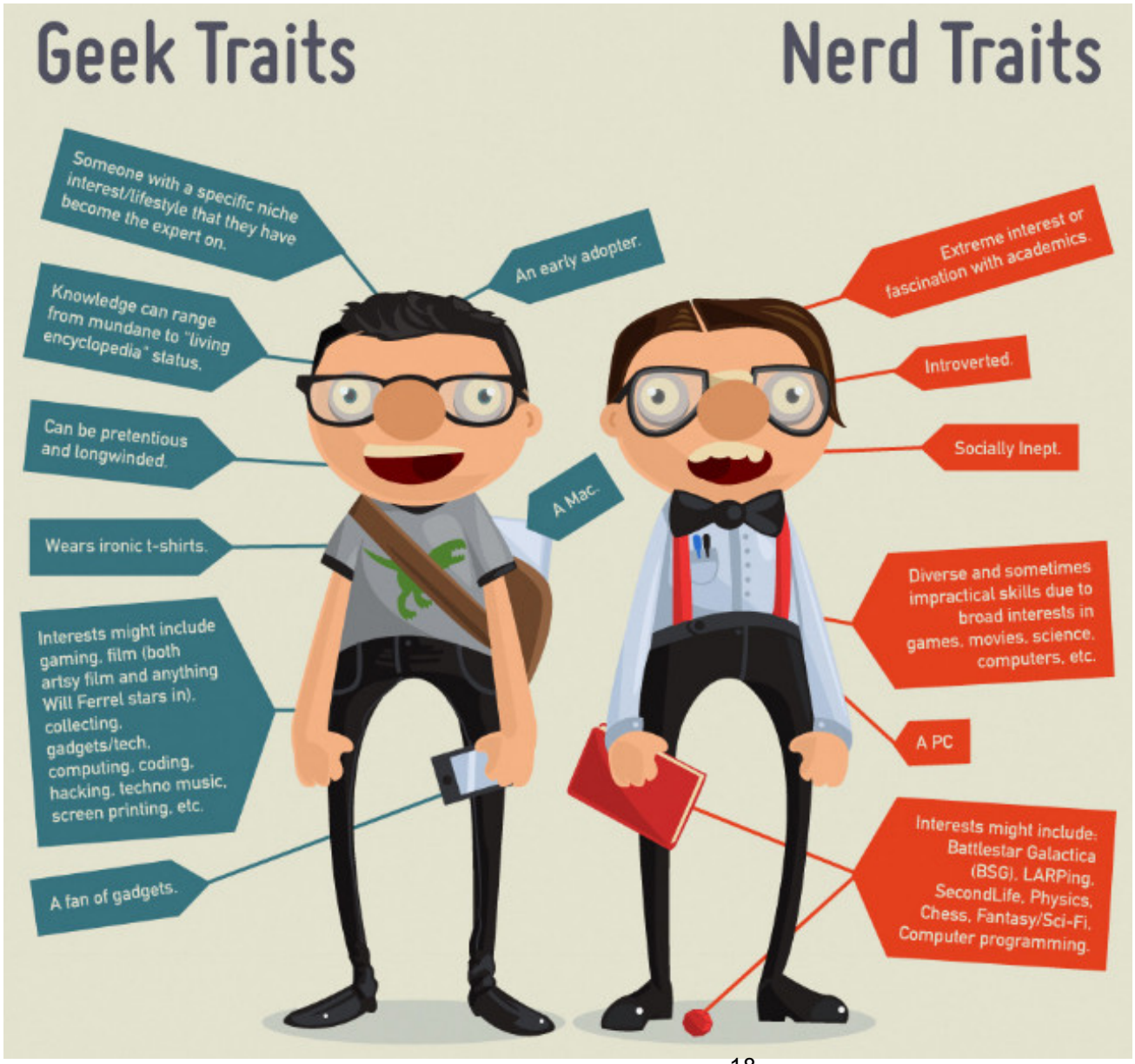
- Up to €10 million, or 2% annual global turnover – whichever is higher.
- Up to €20 million, or 4% annual global turnover – whichever is higher.

The administrative fines are discretionary rather than mandatory; they must be imposed on a case-by-case basis and must be "effective, proportionate and dissuasive".

This fact has given rise to a mushrooming - nay parasitical consultancy industry aimed at managing and reducing risk and charging us for the pleasure.

Never trust Geeks or Nerds

FENWICK ELLIOTT



The construction & energy law specialists

Some stats

FENWICK ELLIOTT

Of the G20 countries the UK has the largest internet economy as a percentage of GDP and we have extended that lead since it was first measured. [My thanks to Department for Digital, Culture Media & Sport, 'A New Data Protection Bill']

.

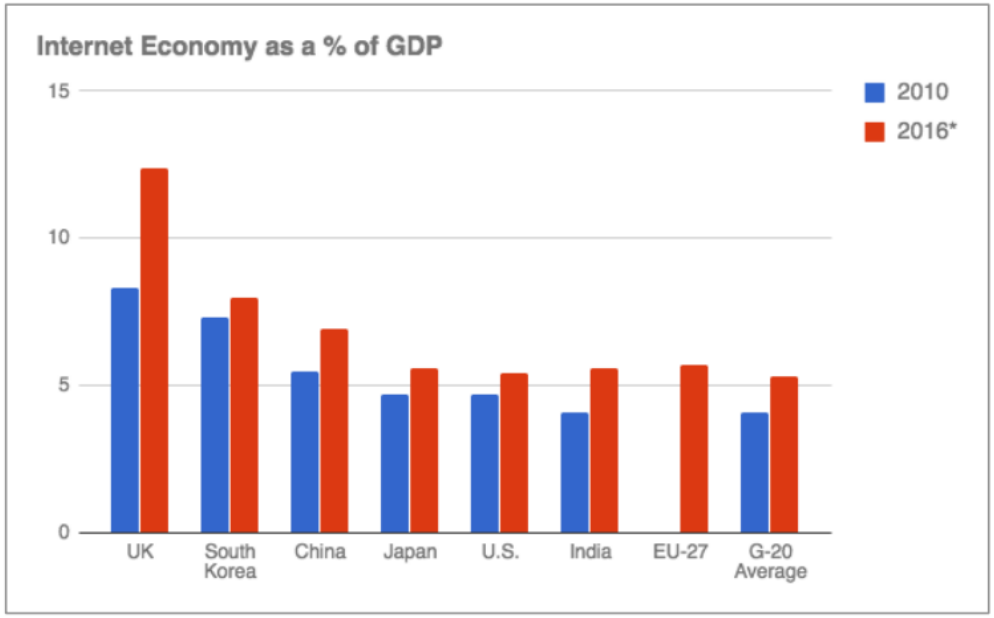


*Fig: BCG Internet Economy in the G-20 Report (2012), * 2016 are projected figures from when it was measured in 2012* [2]

The construction & energy law specialists

Data Protection Registrar - the Information Commissioner's reports are now made public

FENWICK ELLIOTT

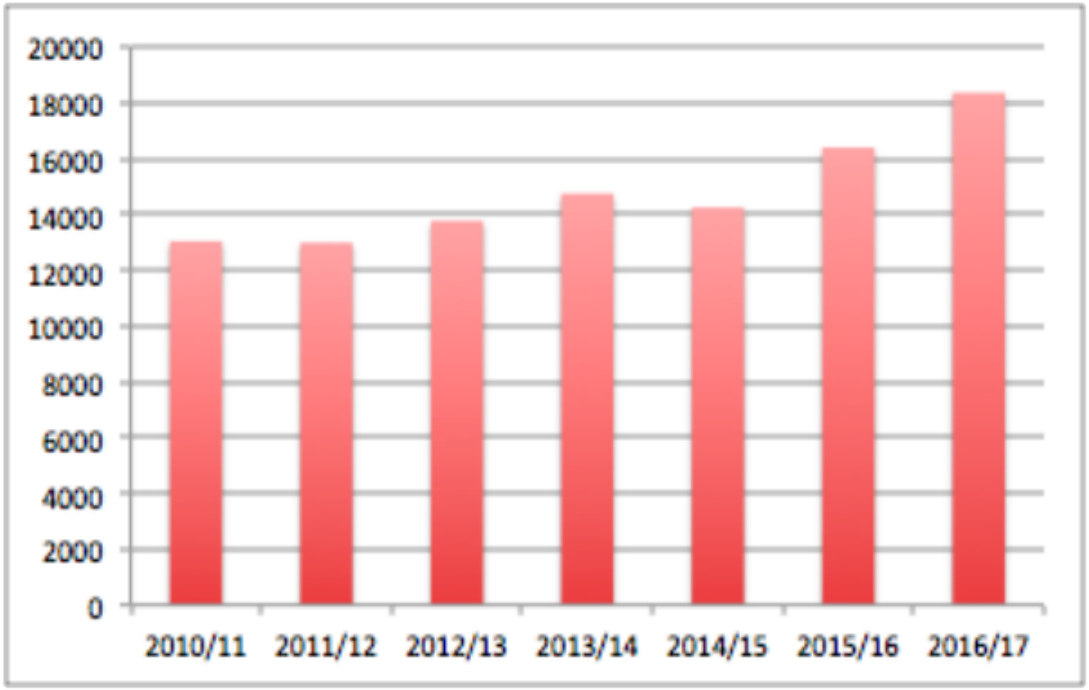


Fig: Data protection concerns received by the Information Commissioner for each financial year (source: ICO annual reports)

The construction & energy law specialists

Fines imposed 1998 to 2018

FENWICK ELLIOTT

The DPA98 provided the legal framework for the use of personal data. In 2010 the IC was given **new teeth with power to enforce fines** and further powers given incrementally, most recently in the **Digital Economy Act 2017**, which made it easier to enforce the law. The DPA needs to be kept up to date to maintain public confidence in the face of "big data" and all the arrays of other technological developments.

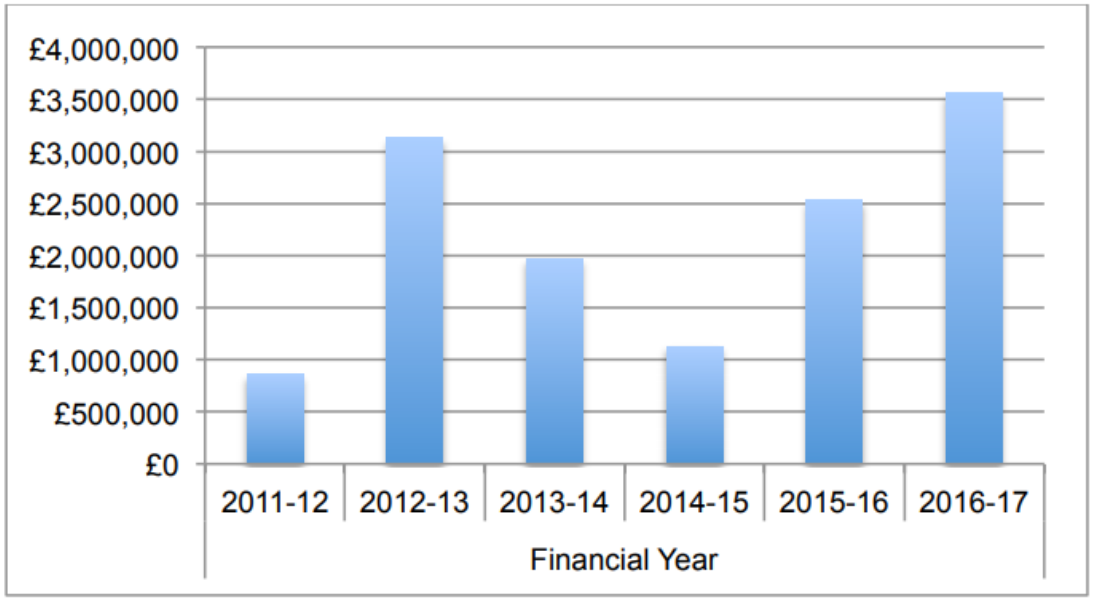


Fig: fines issued by the Information Commissioner under the Data Protection Act and Privacy of Electronic Communication Regulations

The construction & energy law specialists

What's GDPR all about mate?

FENWICK ELLIOTT

It is all about Data protection law and…

- Gives people rights re their personal information.
- Restricts the ways in which organisations can use personal information.

Aims are to:

- Protect people's privacy.
- Harmonise data protection law across EU.
- Update law to reflect developments in IT

The construction & energy law specialists

The protectionist journey started some years ago

FENWICK ELLIOTT

The **Charter of Fundamental Rights of the European Union 2000** enshrines certain political, social, and economic **rights** for **European** Union (**EU**) citizens and residents into **EU** law

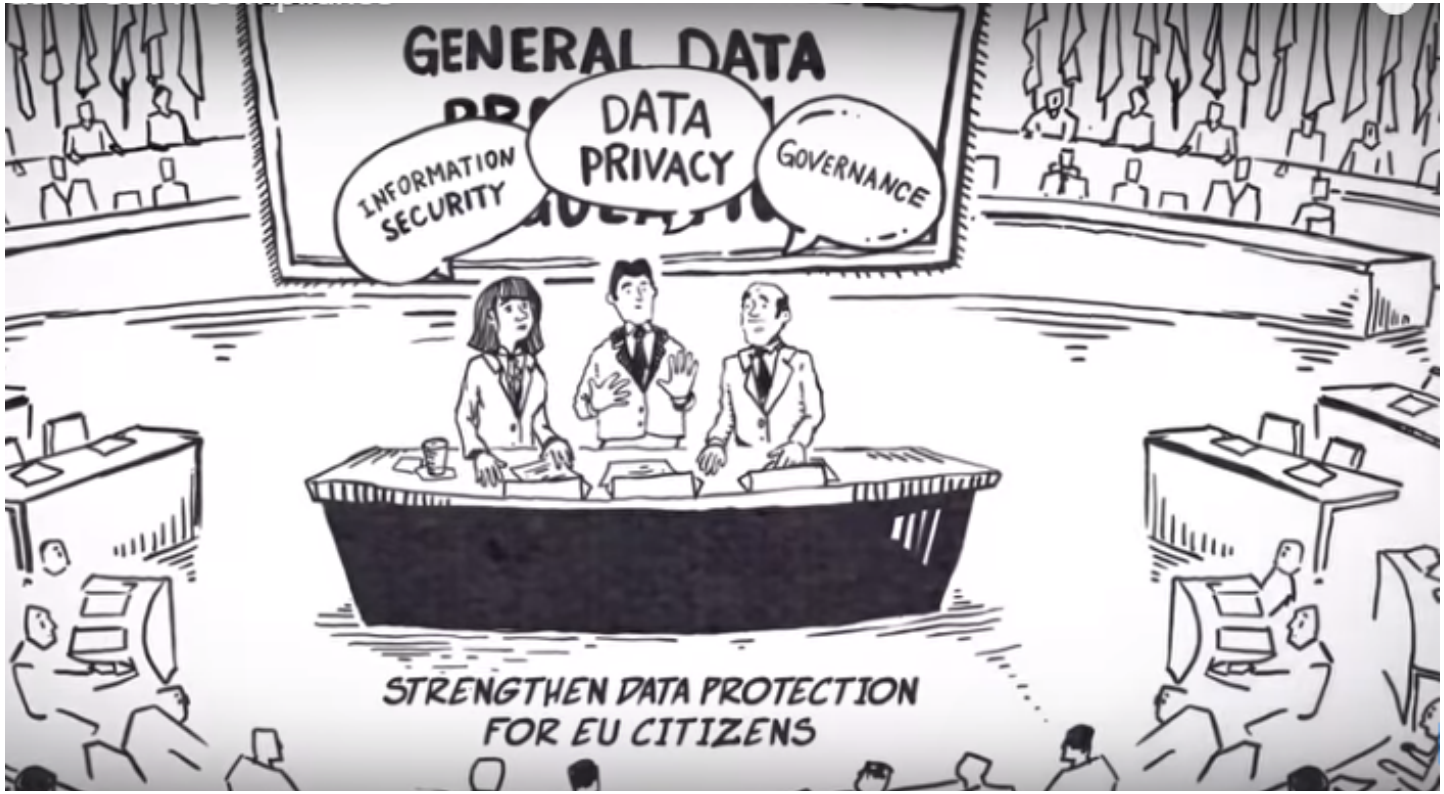
Article 7: Everyone has the *right* to respect for his or her private and family life, home and *communications*.

Article 8 - Right to the protection of personal data

The construction & energy law specialists

The three Amigos

FENWICK ELLIOTT



The construction & energy law specialists

Core principles – Article 5

FENWICK ELLIOTT

Lawful, fair and transparent Article 5(1)(a)	Expected by the person whose data it is Article 5(1)(b)	Just enough data to do what you're doing Article 5(1)(c)	Accurate Article 5(1)(d)	Only kept as long as necessary. Article 5(1)(e)

"processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')"

Article 5(1)(f)

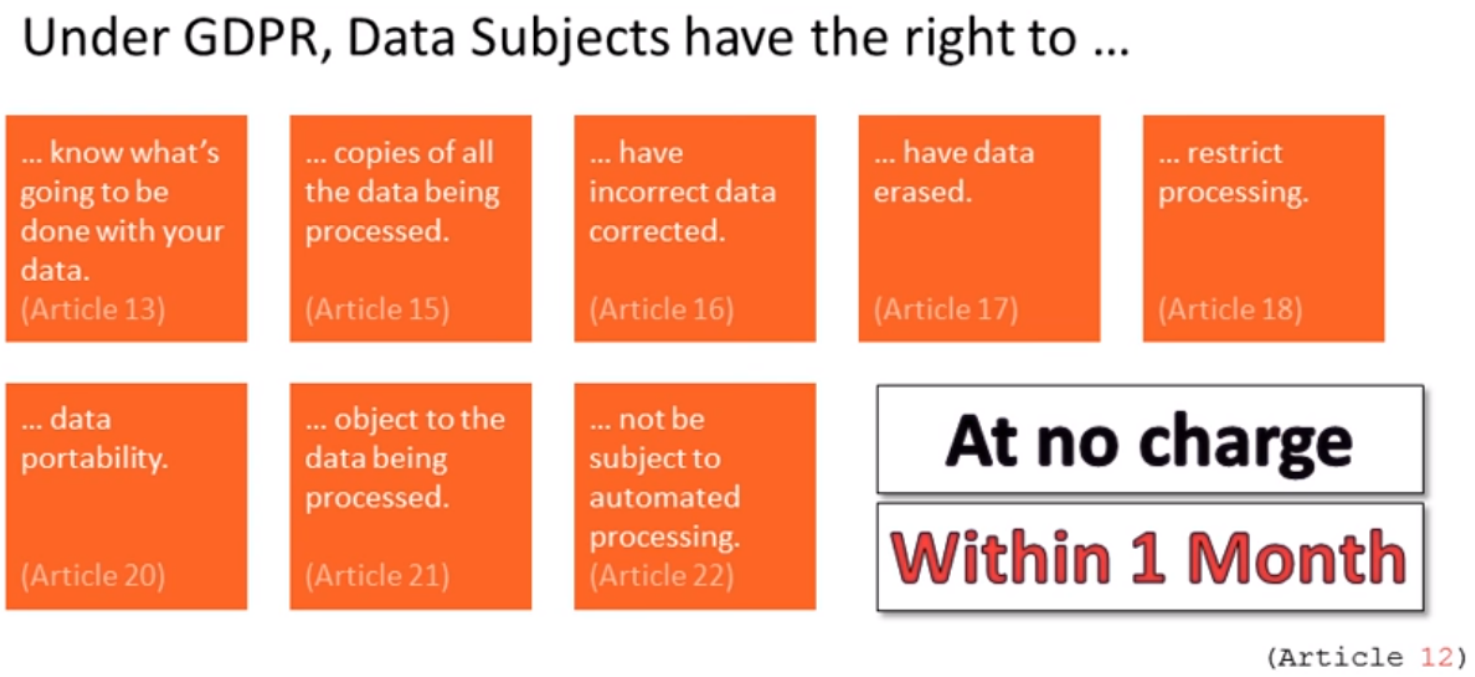
"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')"

Article 5(2)

The construction & energy law specialists

Under the GDPR Data Subjects have these rights, Arts 12 to 22

FENWICK ELLIOTT



The construction & energy law specialists

Data Controllers must, Arts 24 - 33:

FENWICK ELLIOTT

... be accountable, demonstrate compliance (Article 24)

... adopt privacy by design. (Article 25)

... if not in the EU, appoint a representative. (Article 27)

... take care when using third parties (Processors) (Article 28)

... keep records of processing. (Article 30)

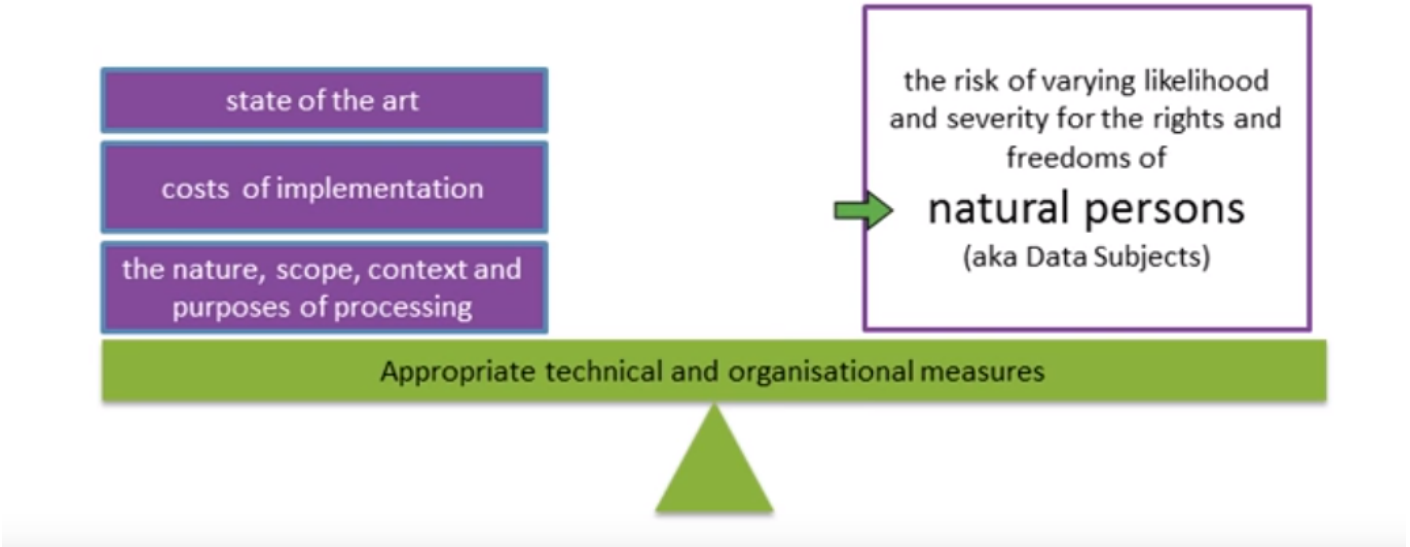
... do security well. (Article 32)

... tell the regulator if they have a breach (72 hrs). (Article 33)

The construction & energy law specialists

…do what to you and me is a risk assessment

FENWICK ELLIOTT



The construction & energy law specialists

State of the Art

FENWICK ELLIOTT

When it comes to GDPR, the ICO realises that not every company can afford the biggest and best products on their network. They do however expect that a company's network has functioning protective products that are suitable for the data stored and that are continuously patched and upgraded.

GDPR – Art 32 – proportionality

FENWICK ELLIOTT

Article 32 of the General Data Protection Regulation (GDPR) requires Data Controllers and Data Processors to implement technical and organizational measures that **ensure a level of data security appropriate for the level of risk presented by processing personal data**. Article 32 specifies that the Data Controller or Data Processor must take steps to ensure that any natural person with access to personal data does not process the data except on instruction of the controller, processor, European Union law, or member state law.

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk …

The construction & energy law specialists

Key words in GDPR

FENWICK ELLIOTT

- Privacy
- Security
- Transparency
- Trust
- Personal data
- Processing
- Data subject
- Controller
- Processor
- Personal data breach

The construction & energy law specialists

Personal data.. What is it?

FENWICK ELLIOTT

Personal data relates to information of an identifier ("*Data subject*") which can be obtained either offline (such as name, location, mental, economic or social identity of a natural person) or online (such as internet protocol address, cookie identity etc). GDPR Articles 4(1), Recital 30.

The construction & energy law specialists

The '*data processor*' *and the* '*data subject*'

FENWICK ELLIOTT

The data processor is *a natural or legal person, public authority, agency or other body* which processes personal data on behalf of the **data controller**, who determines the purposes and means of the processing of personal data.

Solicitors, counsel, or a professional third party such as an expert, arbitral or adjudication institutions/ANBs can be considered data controllers or, in some cases, data processors, thus the GDPR applies potentially to many situations.

The broad definition of "*data subjects*" contained in the GDPR means they a "natural individuals" drill a bit further and every person holding the nationality of a Member State shall be a citizen of the Union (per Article 20 (1) of the Treaty on the Functioning of the European Union)

In the absence of an exemption, GDPR's provisions extend to *the personal data of any individual when the GDPR applies to a data subject*.

Data controllers where are thee

FENWICK ELLIOTT

GDPR applies to all data controllers and data processors who are located in the EU or, if they are not in the EU, who process data of individuals who are in the EU, where the processing activities are related to the offering of services (i.e. arbitration and adjudication) to such data subjects or the monitoring of their behaviour, as long as it takes place within the EU.

The construction & energy law specialists

Power to the people!

FENWICK ELLIOTT

In order to hand power back to the consumer (aka 'data subject' as they're referred to) ensuring compliance has required many businesses (data 'controllers') to make huge changes to how they collect, store and process information.

Reports indicate that many still aren't ready. EY's *Global Forensic Data Analytics Survey 2018* revealed that only one third of global firms are prepared, many watching and waiting.

Power to the people!...

FENWICK ELLIOTT

In order to ensure compliance, **businesses must understand how they interact with third parties**.

Different departments or sectors of a business may typically cooperate with numerous processors, so it's imperative that companies know which unit has granted access to whom, what information is being shared, as well as the types of processing activities being performed. For transparency, contracts should state exactly who is accountable for each specific task in regards to data protection and compliance.

…As for the processors, they are only supposed to use data as instructed by the controllers and to return or delete information once it's fulfilled its intended usage. They cannot sub-contract to an additional third party without written consent from the controller and any that are permitted are again subject to GDPR, as well as the original contract.

The construction & energy law specialists

FENWICK ELLIOTT

Know that businesses are responsible for their third parties !

GDPR holds businesses liable for the actions of third parties ('data processors'). **Article 28** reads *"Where processing is to be carried out on behalf of a controller,* [e.g. eDisclosure platform] *the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject*". Should organisations not follow this and a third party within the network is found to be falling short, they will feel the force of the regulators and will likely be fined.

The construction & energy law specialists

Elizabeth Denham = UK IC

FENWICK ELLIOTT

The message from Elizabeth Denham (IC), - speech on GDPR and accountability for the Institute of Chartered Accountants:

- "*We're all going to have to change how we think about data protection.*"
- *"The GDPR is at root a modernisation of the law."*
- "*Last year we issued more than one million pounds in fines for breaches of the Data Protection Act, so it's not a power we're afraid to use*."
- *"Make no mistake, this one's a game changer for everyone."*

The construction & energy law specialists

Fundamental principles: Personal data shall be:

FENWICK ELLIOTT

1. Processed lawfully, fairly and in a transparent manner
2. Collected for specified, explicit and legitimate purposes
3. Adequate, relevant and limited to what is necessary (aka '*data minimisation*')
4. Accurate and, where necessary, kept up to date
5. Kept for no longer than is necessary
6. Processed in a manner that ensures appropriate security

The construction & energy law specialists


RIGHTS OF DATA
SUBJECTS

The rights of data subjects

FENWICK ELLIOTT

The rights of data subjects [*a data subject is any person whose personal data is being collected, held or processed*] is one of the central areas in the GDPR.

The right for individuals to have access to personal data which is held about them is one of these rights.

The ability of individuals to exercise these rights to obtain copies of their personal data (often referred to as making *a data subject access request* ("DSAR") verbally or in writing) is something which may be either a help or a hindrance to proceedings depending on who you are acting for.

DSAR's lean towards supporting the data subject asking! It must be possible to make DSARs electronically !

The construction & energy law specialists

GDPR - Understanding the eight **rights of** individuals / 'data subjects'

FENWICK ELLIOTT

The **rights** are:

1. **right to** be informed,
2. right **of** access,
3. **right to** rectification,
4. **right to** erasure/to be forgotten,
5. **right to** restrict processing,
6. **right to** data portability,
7. **right to** object **and**
8. **rights in** relation to automated decision making **and** profiling

The construction & energy law specialists

1. The right to be informed

FENWICK ELLIOTT

The right to be informed states how the information you supply about the processing of personal data must be, typically in a privacy notice:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.
- The information you supply is determined by whether or not you obtained the personal data directly from individuals. For more detail and what information you must supply to individuals at what stage

The construction & energy law specialists

2. The right of access

FENWICK ELLIOTT

Under the right of access, you must be able to provide processing confirmation and access to an individual's data free of charge and provide it in a commonly used format - an electronic format if the request is made electronically. Ensure careful planning of this if dealing with multiple systems so you can achieve high efficiency to counter the fact that the information must now be accessed free of charge.

The construction & energy law specialists

3. Right to rectification,

FENWICK ELLIOTT

Individuals are entitled to have their personal data rectified if inaccurate or incomplete and you must respond to a rectification request within one month if not deemed complex. You must inform related third parties where possible if the personal data is disclosed to them also

4. The right to erasure

FENWICK ELLIOTT

The right to be forgotten', or right to erasure means you must have procedures in place for removing or deleting personal data easily and securely where there is no compelling reason for possession and continued processing. Specific circumstances stated by the ICO include:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed. Past Decisions of adjudicator? But what about professional retention policy?
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (i.e. otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

5. The right to 'block' or restrict processing

FENWICK ELLIOTT

Individuals have the right to 'block' or restrict processing of personal data, in the following circumstances outlined by the ICO:

- "Where an individual contests the accuracy of the personal data, you should restrict the processing until you have verified the accuracy of the personal data."
- "Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and you are considering whether your organisation's legitimate grounds override those of the individual."
- "When processing is unlawful and the individual opposes erasure and requests restriction instead."
- "If you no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim."
- You must inform any third parties that are also involved with the data about the restriction, and inform individuals when you remove a restriction on processing.

6. The right to data portability

FENWICK ELLIOTT

The right to data portability allows individuals to obtain and reuse their personal data across different services for their own purposes. The right only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is automated.
- The right allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting usability. Personal data must be provided in a structured, commonly used and machine readable format so other organisations can use it, and must be provided free of charge.

7. The right to object

FENWICK ELLIOTT

The right to object means individuals have the right to object to **direct marketing** (including profiling), processing based on legitimate interest, and purposes of scientific/historical research and statistics, in which case you must stop processing personal data immediately and at any time, with no exemptions or grounds to refuse, free of charge.

Ensure you are informing individuals of their right to object in your privacy notice and "at the point of first communication". If you process personal data for research purposes, or for the performance of a legal task or your organisation's legitimate interests, see further details here. If your processing activity is one of the above and carried out online you must offer the option to object online, e.g. through your website.

8. Rights related to automated decision making

FENWICK ELLIOTT

If any of your processing operations constitute automated decision making including profiling (such as insurance firms), individuals have the right not to be subject to a decision and must be able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it. The right does not apply if the automated decision is a contractual necessity between you and the person, if it's authorised by law, or if based on explicit consent.

Personal data breach - PDBs

FENWICK ELLIOTT

Article 33: 'Personal data breach' means *the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.*

The construction & energy law specialists


RIGHTS OF DATA
SUBJECTS

The rights of data subjects

FENWICK ELLIOTT

The rights of data subjects is one of the central areas in the GDPR.

The right for individuals to have access to personal data which is held about them is one of these rights.

The ability of individuals to exercise these rights to obtain copies of their personal data (often referred to as making *a data subject access request* ("DSAR") verbally or in writing) is something which may be either a help or a hindrance to proceedings depending on who you are acting for.

DSAR's lean towards supporting the data subject asking! It must be possible to make DSARs electronically !

The construction & energy law specialists

Adjudicators and arbitrators

FENWICK ELLIOTT

Taking account of the fact, solicitors, counsel, or a professional third party such as an expert, or an arbitral or adjudication institution / ANB can be considered data controllers or, in some cases, data processors, the GDPR applies potentially to many situations.

GDPR may affect how an adjudicator or for that matter party representative gather documents to establish the facts of a case. While there are legal bases which allow for a proper processing of data without obtaining consent (e.g. legitimate interest), you in this room as practitioners will have to be aware and read up on these bases. Likewise, arbitration and adjudication may well involve documents from third parties, and solicitors, counsel, party reps may have to deal with the processing of their personal data, too.

Adjudicators and Arbitrators / Tribunals and arbitral and adjudication institutions (in addition to companies selling arbitration databases) will have to ensure compliance with the GDPR.

Adjudicators and arbitrators…

FENWICK ELLIOTT

As the recipients of data, tribunals will have the task of complying with one of the six different legal bases for the processing of personal data and respect the rights of the data subjects.

The right of access, which is almost absolute, poses a particular challenge as a tribunal cannot in principle object to a request from an individual to see what information it has on him or her. Tribunals must also ensure that data is adequately protected.

The GDPR also poses challenges for institutions which keep databases on cases (e.g. ICSID) and adjudicators and arbitrators. It could be possible that miffed arbitrator or adjudicator, for example, might ask for access to the institution's data following a challenge or might request to see a firm's data on him or her to ascertain why he or she was not appointed in a particular case.

All those parties involved should prepare their *Record of Processing Activities* and include with all detail the specific contents established in the GDPR.

GDPR and *disclosure* of documents

FENWICK ELLIOTT

The concern is the extent to which EU data protection rules might affect *disclosure* of documents in *arbitration* (and to a rather lesser extent the impact of GDPR on the practice of adjudicators and adjudication proceedings).

This audience knows there is no 'disclosure' in HGCRA/LDEDCA adjudication as we know it in court or arbitration. But the recent Mr Jonathan Acton Davis QC decision in *Vinci Construction UK Ltd v Beumer Group UK Ltd* [2018] the seventh adjudication between the parties, may change that ever so slightly…(re failure to disclose material) and a NJ point.

The judge found that the adjudicator did not order disclosure because he was not requested to do so and that nothing was put before him that would have required him to make such an order.. But one can see where this may be heading, particularly under TeCSA Sub-rule 18.2 and 18.3.

TeCSA Sub-rule 18.2 and 18.3

FENWICK ELLIOTT

18.2 Require any Party to produce a bundle of key documents, whether helpful or otherwise to that Party's case, and to draw such inference as may seem proper from any imbalance in such bundle that may become apparent…

18.3 Require the delivery to him and/or the other Parties of copies of any documents other than documents that would be privileged from production to a court…

The construction & energy law specialists

GDPR and disclosure in Court but what of beyond?...

FENWICK ELLIOTT

The definition of "personal data" for the purposes of GDPR law is very broad. It is broader than US law and certainly broad enough to catch some of the documents that would routinely be disclosed in litigation or arbitration.

For example, email negotiations carried out by an employee of a company with a third party might well constitute the "personal data" of that employee or third party and, therefore, subject to the constraints imposed by the GDPR. Similarly, the broad definition of "processing" under GDPR law would certainly encompass the application of a litigation hold and all aspects of the performance of disclosure.

The construction & energy law specialists

GDPR and disclosure in Court but what of beyond?...

FENWICK ELLIOTT

This means that the performance of discovery obligations in litigation or arbitration may be, prima facie, inconsistent with EU law data protection constraints on the processing and transfer of data.

What is to happen if a party to litigation is ordered to disclose documents that are subject to data protection constraints? In the context of English court litigation, we shall see any contradiction is addressed by the provision in the GDPR recognising that processing of data is lawful where it is **necessary to comply with a legal obligation**, including a court order to disclose documents.

However, no such legal obligation arises from arbitration, or adjudication which in the case of arbitration is consensual and in which the arbitrator's directions give rise to contractual, or perhaps quasi-contractual, obligations. In Adjudication it is statutory and contractual and consensual too. [We will need some case law!]

The construction & energy law specialists

GDPR and disclosure in Court but what of beyond?...it is all new!

FENWICK ELLIOTT

I strongly suspect that disclosure obligations in arbitral proceedings (and on very rare occasion adjudication) will probably **fall within a further ground of lawfulness provided for in the GDPR: *that the processing is necessary for the purposes of legitimate interests pursued by the data controller***.

However, this is a much more fluid and nebulous ground, and may be displaced where the interests of the individual data subject outweigh those legitimate interests. REMEMBER the general scheme of the GDPR is to require processing to be **limited to that which is proportionate and necessary to achieve the stated purpose**. This introduces a still further level of nuance and fluidity in arbitration.

It suggests, for example, that **it may no longer be acceptable to search for, collate, and disclose all "relevant" documents. Instead, considerations of proportionality may point towards a more focused process of identification, assessment and weighing**, in order to ensure that data protection obligations are not breached.

By the by Standard Disclosure will die and it is dying anyway. The **impending Disclosure Pilot (starting this month)** for the Business and Property Courts **will I am sure be soon law !**

BUT – me thinks the lack of disclosure process in adjudication makes it far less relevant to worry about as processing will generally limited.

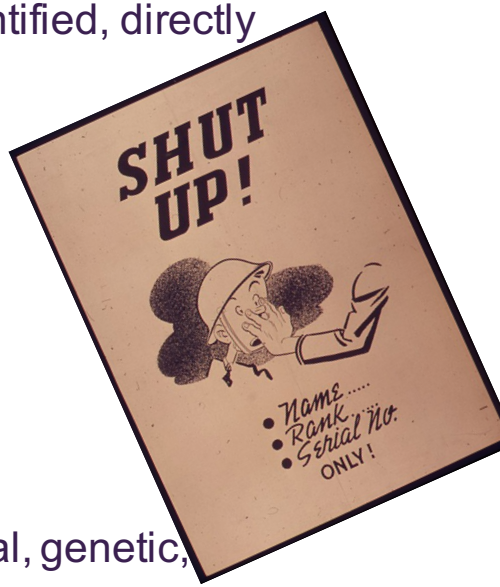
The construction & energy law specialists

What you do as an adjudicator with data ?

FENWICK ELLIOTT

What may be more relevant is <u>what you as an adjudicator do with data you process</u> if it concerns the **processing** of '**personal data**', which is defined as '*any information relating to an identified or identifiable natural person'*.

An identifiable natural person is defined as a person 'who can be identified, directly or indirectly, in particular by reference to an identifier such as a:



- name,
- an identification number,
- location data,
- an online identifier
- or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.

The construction & energy law specialists

Lawyers eye view

FENWICK ELLIOTT

As a lawyer the GDPR (for example) requires me to tell the data subject

- who I am,
- how that person can contact me about their personal data,
- for what purposes I may process their personal data and
- the legal basis for doing so,
- the people with whom I may share their personal data,
- the circumstances in which I may transfer their personal data outside the UK and/or the EU, the period for which I will store their personal data and the criteria I use for deciding how long to retain this personal data of theirs.
- The GPDR also requires me to tell the person how they can request access to and rectification or erasure of their personal data, how to make a complaint etc.

How I may use your personal data

FENWICK ELLIOTT

I may use your personal data for the following purposes:

- to provide legal services to my clients, the provision of legal advice and representation in courts, **tribunals, adjudications**, **dispute boards, arbitrations**, settlement negotiations and mediations, or **when acting as an arbitrator, adjudicator, mediator** or dispute board member;
- to keep accounting records and carry out administration of my practice;
- to take or defend legal or regulatory proceedings or to exercise a lien;
- to respond to potential complaints or make complaints;
- to check for potential conflicts of interest in relation to future potential cases;
- to promote and market my/firm services;
- to carry out anti-money laundering and terrorist financing checks;
- to train other solicitors and when providing work-shadowing opportunities;
- to respond to requests for references;
- when procuring goods and services;
- to publish legal judgments and decisions of courts and tribunals; and as required or permitted by law.

With whom might I share it?

FENWICK ELLIOTT

It may be necessary to share information with the following:

- Data processors, such as my staff, eDisclosure providers, IT support staff, email providers, data storage providers, my PA, my personal administrator and accountant;
- Other legal professionals, including trainees assisting me on a matter;
- Experts and other witnesses;
- Prosecution authorities in the UK or otherwise;
- Courts and tribunals;
- In the event of complaints, my Partners/Members and staff who deal with complaints, the SRA, and the Legal Ombudsman,
- Other regulatory authorities,
- Business associates, professional advisers and trade bodies, e.g. the Law Society and SRA.
- The intended recipient, where you have asked me to provide a reference, and
- The general public in relation to the publication of legal judgments and decisions of courts and tribunals

Legal professional privilege

FENWICK ELLIOTT

If this exemption pursuant to Article 23 and (Schedule 2 para 19) of DPA18 applies and if you process personal data: to which a claim to legal professional privilege could be maintained in legal proceedings; or in respect of which a duty of confidentiality is owed by a professional legal adviser to his client.

It exempts you from the GDPR's provisions on:

- the right to be informed;
- the right of access;
- and all the principles, but only so far as they relate to the right to be informed and the right of access.

http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/enacted

GDPR and Solicitors and Claims Consultants

FENWICK ELLIOTT

Like any other professional or commercial organisation, a solicitors' firm (ditto a claims management consultant etc) may face data subject access requests from aggrieved or merely inquisitive individuals. Like other such organisations, the firm may as a result have concerns about the confidentiality of its own internal processes in relation to matters such as client complaints, whistle-blowing investigations, grievance and disciplinary procedures, partnership disputes, and the like.

Uniquely a solicitors' firm will typically hold large amounts of privileged and/or confidential information about its clients.

That not only increases the likelihood of subject access requests being made by third parties, but also makes such requests more difficult to handle.

Too early yet to say how this will work out but we are already hearing noises about DARs.

Potential grounds of resistance… reason to be cheerful?

FENWICK ELLIOTT

Where a firm acts for a client in litigation, and it receives a subject access request made by that client's opponent in the litigation, the firm's natural reaction to the request is likely to include all or some of the following (in increasingly plaintive tones):

- "Ask our client, not us" (the firm's status as agent)
- "But our file's privileged" (legal professional privilege)
- "But our file's confidential" (the firm's obligation of confidentiality)
- "But that's not what data protection is for" (collateral purpose)
- "But that's going to be a nightmare for us to deal with" (disproportionality)
- "But that's really unreasonable and unfair" (abuse of process/rights)
- "But surely the Court's not going to make us answer that?" (the Court's discretion)

These understandable objections have met with only mixed success under two recent decisions of the Court of Appeal.

Potential grounds of resistance…

FENWICK ELLIOTT

The firm's status as agent

The Court of Appeal disposed briefly of the first objection in *Dawson-Damer v Taylor Wessing LLP* [2017] 1 WLR 3255, at [55], under the heading, "*Fact that TW are the trustee's solicitors of little relevance*":

There is no conceptual difficulty under the DPA arising from the fact that TW is an agent. The critical point is that TW is a data controller.

Potential grounds of resistance…

FENWICK ELLIOTT

Legal professional privilege

Notwithstanding para 19 of Part 4 of Schedule 2 to the DPA18, subject access rights do not apply to:

...personal data that consists of information in respect of which a claim to legal professional privilege... could be maintained in legal proceedings.

BUT leaving aside the difficulties in applying to *information* a legal principle which has been developed in relation to *documents*, a solicitor's file will typically contain much unprivileged information. In *Ittihadieh v 5-11 Cheyne Gardens RTM Co Ltd* [2018] QB 256, at [102], Lewison LJ said:

"If some personal data are covered by legal professional privilege and others are not, the data controller will have to carry out a proportionate search to separate the two."

Potential grounds of resistance…

FENWICK ELLIOTT

The firm's obligation of confidentiality

Mere confidentiality is not a complete bar to a subject access request, but the right to access (of X) is qualified if the data is also the personal data of a third party (Y). Under paragraph 16 of Part 3 of Schedule 2 to the DPB18.

This exemption (which does not appear to have been directly in issue before the Court of Appeal in either *Dawson-Damer* or *Ittihadieh*) is naturally likely to have a more pervasive effect when the solicitor's client (Y) is an individual, rather than a corporation. In *Ittihadieh*, at [101], Lewison LJ observed that:

...whether it is reasonable to disclose information about another individual (Y) is an evaluative judgment which must, as it seems to me in the current state of technology, be carried out by a human being rather than by a computer.

Potential grounds of resistance…

FENWICK ELLIOTT

Collateral purpose

The Court of Appeal in both *Dawson-Damer* (at [105] to [114]) and *Ittihadieh* (at [86] to [89]) rejected the submission that a subject access request was invalid if it was made with a collateral purpose, such as litigation.

Disproportionality

The judgments in *Dawson-Damer* and *Ittihadieh* are not encouraging for solicitors seeking to reject a subject access request outright on the basis that it is disproportionate, but they both confirm that principles of proportionality apply implicitly to the burdens of search, analysis and production which are imposed by a request (*Dawson-Damer*, at [74] to [79]; *Ittihadieh*, at [95] to [103]).

In *Gaines-Cooper v Commissioners for HMRC* [2017] EWHC 868 (Ch) HHJ Jarman QC held that HMRC, which had made significant efforts to comply with a subject access request, had done enough to comply with its obligations, even though significant quantities of potentially relevant documentation remained unexamined.

Abuse of process/abuse of rights

In *Dawson-Damer*, at [109], the Court of Appeal raised the possibility that an application to enforce rights of access might in some circumstances amount to an abuse of process, and this possibility was confirmed in *Ittadieh*, at [88]. The Court of Appeal suggested in the latter case that there was not much difference between the domestic concept of abuse of process and the EU doctrine of "abuse of rights".

Potential grounds of resistance…

FENWICK ELLIOTT

The Court's discretion

In *Ittihadieh*, at [104] to [110], the Court of Appeal considered the nature of the Court's discretion on applications by data subjects to enforce their access rights. It held that if a data controller had failed to conduct a proportionate search in response to a valid request then, absent other material factors, the Court's discretion should usually be exercised in favour of the data subject.

However, the Court of Appeal also identified a number of factors which are of potential relevance to the Court's exercise of its discretion, including:

- whether there is a more appropriate route to obtaining the requested information
- the nature and gravity of the data controller's breach
- whether there is a legitimate reason for making the access request
- whether an abuse of rights is involved
- whether the application is procedurally abusive
- whether the real quest is for documents, rather than personal data
- whether the personal data is of no real value to the data subject
- whether the data subject has already received the data

The Court of Appeal stated that this list was not intended to be prescriptive, but it is likely to be the subject of close examination on many future applications

Six different legal bases for the processing of personal data

FENWICK ELLIOTT

As the recipients of data, as a tribunal member or as an adjudicator you will have the task of complying with one of the six different legal bases for the processing of personal data and respect the rights of the data subjects.

The data subjects right of access, which is almost absolute, poses a particular challenge as a tribunal cannot in principle object to a request from an individual to see what information it has on him or her. Tribunals must also ensure that data is adequately protected.

The construction & energy law specialists

The 6 legal bases…

FENWICK ELLIOTT

Of the six available lawful bases for processing :

- No single basis is 'better' or more important than the others
- Most lawful bases require that processing is 'necessary'
- Except 'consent'…

The construction & energy law specialists

The 6 bases - personal data processing is lawful only when (and to the extent that) it is permitted under applicable law

FENWICK ELLIOTT

1. Compliance with a legal obligation
2. Contractual performance
3. Vital interests
4. Public interest or acting under official public authority
5. Legitimate interests
6. Data subjects' consent

The construction & energy law specialists

…Compliance with a legal obligation

FENWICK ELLIOTT

The most stringent and precise basis, but also the optimal basis for processing (with respect to the data controller) is the existence of at least one legal provision demanding (i.e., justifying) the processing activities.

In short, when you are obliged to process the personal data to comply with the law it is okay to do so. Acting in a quasi judicial capacity should be good enough!

Article 6(3) requires that the legal obligation must be laid down by UK or EU law. Recital 41 confirms that this does not have to be an explicit statutory obligation, as long as the application of the law is foreseeable to those individuals subject to it. So it includes clear common law obligations.

This does not mean that there must be a legal obligation specifically requiring the specific processing activity. The point is that your overall purpose must be to comply with a legal obligation which has a sufficiently clear basis in either common law or statute.

…Contractual performance

FENWICK ELLIOTT

You can rely on this lawful basis *contractual performance* if you need to process someone's personal data:

- to fulfil your contractual obligations to them, such as contractual adjudication; or

- because they have asked you to do something before entering into a contract (e.g. provide a quote).

The processing must be necessary. If you could reasonably do what they want without processing their personal data, this basis will not apply.

The construction & energy law specialists

Vital interests

FENWICK ELLIOTT

You are likely to be able to rely on vital interests as your lawful basis if:

- you need to process the personal data to protect someone's life (unlikely to arise as a humdrum adjudicator).

- The processing must be necessary. If you can reasonably protect the person's vital interests in another less intrusive way, this basis will not apply.

- You cannot rely on vital interests for health data or other special category data if the individual is capable of giving consent, even if they refuse their consent.

If you rely on this basis you must document the circumstances where it will be relevant and ensure you can justify your reasoning.

Public interest or acting under official public authority

FENWICK ELLIOTT

You can rely on this lawful basis if you need to process personal data:

- 'in the exercise of official authority' such as a magistrate, judge or coroner. This covers public functions and powers that are set out in law; or

- to perform a specific task in the public interest that is set out in law.

It is most relevant to public authorities, but it can apply to any organisation that exercises official authority or carries out tasks in the public interest.

You do not need a specific statutory power to process personal data, but your underlying task, function or power must have a clear basis in law.

If an organisation is holding personal data to support research, it is highly likely that it will also be required to apply appropriate 'technical and organisational measures', in order to have access to specific research exemptions provided in GDPR and the new Data Protection Act.

The construction & energy law specialists

Legitimate interests

FENWICK ELLIOTT

'*Legitimate interests'* is the most flexible lawful basis for processing, but you cannot assume it will always be the most appropriate.

Processing is necessary for the purposes of the legitimate interests except where such interests are overridden by the interests or fundamental rights and freedoms of the individual which require. Protection of personal data, in particular where the individual is a child. Again not too relevant to those in this audience.

The construction & energy law specialists

Data subjects' consent

FENWICK ELLIOTT

The GDPR sets a high standard for consent.

Under the GDPR, consent must be "freely given, specific, informed and unambiguous."

Affirmative action signalling consent may include ticking a box on a website, "choosing technical settings for information society services," or "another statement or conduct" that clearly indicates assent to the processing. "Silence, pre-ticked boxes or inactivity," however, is presumed inadequate to confer consent.

If consent is difficult, look for a different lawful basis. Consent means offering individuals real choice and control.

The construction & energy law specialists

Consent…

FENWICK ELLIOTT

"Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"

Emphasis is on individuals having clear choices and ongoing control over their consent.

The construction & energy law specialists

List of the legal grounds we rely on – example for a party representative

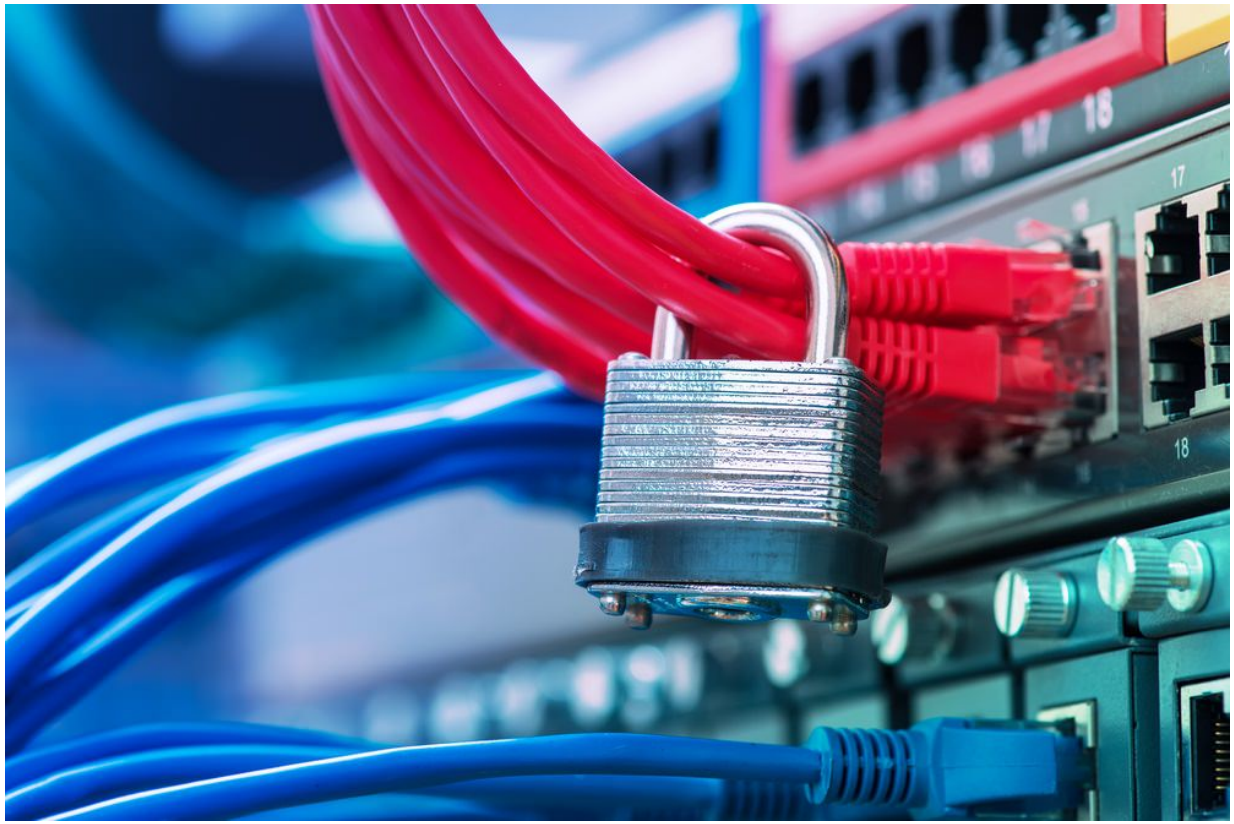
FENWICK ELLIOTT

For processing Personal Data and special categories of Personal Data	
Legal ground	Details
Performance of our contract with you	Processing is necessary for the performance of a contract to which you are party or in order to take steps at your request prior to entering into a contract.
Compliance with a legal obligation	Processing is necessary for compliance with a legal obligation to which we are subject.
For our legitimate business interests	Processing is necessary for the purposes of the legitimate interests pursued by us or by a third party, except where such interests are overridden by your interests or fundamental rights and freedoms which require protection of Personal Data, in particular where you are a child. These legitimate interests are set out next to each purpose.
For processing special categories of Personal Data	
Your explicit consent	You have given your explicit consent to the processing of the Personal Data for one or more specified purposes. You are free to withdraw your consent, by contacting our Data Protection Contact. However, withdrawal of this consent may impact our ability to provide the services. For more detail see the Consent section above.
For legal claims	Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
Substantial public interest	Processing is necessary for reasons of substantial public interest, on the basis of EU or UK law, including where such processing is necessary for insurance purposes or fraud prevention purposes.

The construction & energy law specialists

Day to day life on dispute resolutionists

FENWICK ELLIOTT



The construction & energy law specialists

“Shared folders” and SharePoint and OneDrive

FENWICK ELLIOTT

- THINK!

- Do we restrict access to only those that require it?
- When did we last check the permissions on these folders?

The construction & energy law specialists

USB

FENWICK ELLIOTT

THINK!

- High risk!
- 32GB of data – which can be transferred/taken home
- *Morrisons* supermarket case
- Do you really *need* them?
- 'Lock down' and restrict usage to limited number of computers
- Encryption

The construction & energy law specialists

Papyrus, Vellum, Parchment, Paper,

FENWICK ELLIOTT

- THINK!
- Are you still using paper files?
- Where are these stored?
- Who has access to them?
- Are they left on desks or in boxes in the open plan office?

The construction & energy law specialists

Outsourced and third parties

FENWICK ELLIOTT

- Processing carried out *on your behalf* by a third party

MUST:

- Only use organisations that provide sufficient security and
- Have written contract with GDPR-compliant T&Cs

THINK!

- About those that you/your team use
- Do you have a contract with them?
- Have you checked it complies with GDPR?

The construction & energy law specialists

GDPR after we exit European Union

FENWICK ELLIOTT

The construction & energy law specialists

GDPR after we exit European Union…

FENWICK ELLIOTT

GDPR will no longer directly apply to organisations in the UK, and UK citizens will no longer be considered EU citizens so will not be extended the same protections GDPR offers to EU citizens.

After 29 March 2019, parliament will be able to make changes to the GDPR framework as it sees fit. Hoorayyyy! Boooo etc

According to the regulations themselves, the transfer of personal data to a non-EU country is prohibited unless that country has "*an adequate level of data protection*". The UK can ensure it meets that "adequate level" by maintaining GDPR's rules, hence DPA18 – we hope!

Post-Brexit, the UK won't be subject to decisions by both European Court of Justice and of the European Board of Data Protection. In addition, the UK Information Commissioner's Office (ICO) will no longer participate in the European Data Protection Board, losing influence on interpretations of law and decisions within the EU.

GDPR after we exit European Union …

FENWICK ELLIOTT

Official line:

GDPR applies to all companies based in the EU and those with EU citizens as customers. It has an extraterritorial effect, so non-EU countries are also affected. Even though the UK is planning to leave the EU, the UK will still need to comply with the GDPR.

Until exit negotiations are concluded, the UK remains a full member of the European Union and all the rights and obligations of EU membership remain in force.

Ceteris paribus, and we gave the answer on 23 June 2016, come 29 March 2019 GDPR will not be directly applicable.

Practically for domestic adjudicators in England and Wales this may make GDPR a bit of a dead duck. But on the wider stage international companies across the globe with any EU citizens as customers will need to heed their legal obligations and comply to avoid fines.

But there is a fly in the ointment, the Data Protection Act 2018

The construction & energy law specialists

GDPR after we exit European Union …

FENWICK ELLIOTT

When the UK leaves the European Union, whilst theoretically be free from the laws set by Brussels and the GDPR and all of its aspects could be struck from British laws through the *great repeal bill*, never to be seen or heard of again on these shores **UK businesses in this scenario would be faced with the prospect of transferring data to the US and the EU operating under drastically differing guidelines**. That fly again!

Ratbags you might say!

The Data Protection Act 2018 is effectively our domestic GDPR. To ensure (the aim anyway) that British organisations can continue to trade and share data with EU counterparts after Brexit, the Government made moves to absorb GDPR's requirements into UK law. The existing 'Data Protection Act 1998' was repealed and replaced by the 2018 Act.

But the DPA18 is necessarily incomplete and must be interpreted in conjunction with the text of the GDPR**.** Where there are no specific provisions or derogations contained within the DPA18, the GDPR's text applies. For example, Article 37(1) specifies the conditions under which it is necessary to appoint a DPO, a matter on which the DPA remains silent.

So query how complete our law is post April 2019. Concern still exists in EU member countries regarding UK mass surveillance techniques and the use of data by UK intelligence agencies…So nobody really knows.

GDPR after we exit European Union …

FENWICK ELLIOTT

The DPA18 is thus what lawyers call *lex specialis*, i.e. the specialising law for the UK in respect to personal data protection.

Whilst the EU wants the European Court of Justice (CJEU) to represent the court of final appeal for all decisions on data protection. The UK will not now be bound by this court's authority, which will mark my words lead to a conflict!

Another concern of EU lawmakers is how the GDPR may develop and change over time, as laws are often amended. There is no mechanism built into the UK Data Protection Act (2018) to automatically include such changes as they occur. More tension…

The UK has long had a special relationship with US, especially in the areas of intelligence sharing and law enforcement purposes. The introduction of laws such as the US CLOUD Act may undermine provisions of GDPR in the minds of EU regulators, leading to potential conflicts about the lawful basis for 3rd country (yes we would be one) transfer mechanisms, especially in light of the legal challenges of the EU/US Privacy Shield — a mechanism that in any case will no longer apply to the UK after Brexit, requiring the establishment of a new UK/US Privacy Shield at the least.

Investigatory Powers Act 2016 aka the "Snooper's Charter" rows the other way

FENWICK ELLIOTT

Parliament has also enacted the **Investigatory Powers Act 2016** (nicknamed the "Snooper's Charter") which allows broad interception, interference and communications powers and limits the rights of individuals under EU law. It has also refused to incorporate the Charter of Fundamental Rights of the EU that provides fundamental privacy rights alongside the GDPR.

The GDPR constitutes the most comprehensive enhancement of individual digital rights and reform of digital customer protection law that the UK has seen so far. However, its enactment in the UK looks to frustrate the application of the controversial Investigatory Powers Act.

That Act slams into Article 17 of GDPR re Right to erasure ('**right to be forgotten**') - one of the most (in)famous aspects. Data subjects have the right to have their personal data removed from the systems of controllers and processors under a number of circumstances, such as by removing their consent for its processing.

The GDPR Right to Erasure

FENWICK ELLIOTT

Not quite as simple as it first appears.

- Article 17 of the GDPR states that data subjects have the right to have their personal data removed from the systems of controllers and processors under a number of circumstances, such as by removing their consent for its processing

- complying with this is a daunting task, and to add to the complexity, there are many cases where conflicting regulations will prevent the processor from complying with the request.

The construction & energy law specialists

The GDPR Right to Erasure...

FENWICK ELLIOTT

The Requirements

Article 17 of the GDPR, The Right To Erasure, states:

Data Subjects have the right to obtain erasure from the data controller, **without undue delay**, **if** one of the following applies:

- The controller doesn't need the data anymore
- The subject withdraws consent for the processing with which they previously agreed to (and the controller doesn't need to legally keep it [N.B. Many will, e.g. banks, for 7 years.])
- The subject uses their right to object (Article 21) to the data processing
- The controller and/or its processor is processing the data unlawfully
- There is a legal requirement for the data to be erased
- The data subject was a child at the time of collection (See Article 8 for more details on a child's ability to consent)
- If a controller makes the data public, then they are obligated to take reasonable steps to get other processors to erase the data, e.g. A website publishes an untrue story on an individual, and later is required to erase it, and also must request other websites erase their copy of the story

The GDPR Right to Erasure...

FENWICK ELLIOTT

Exceptions

Data might not have to be erased if any of the following apply:

The “right of freedom and expression”

The need to adhere to legal compliance, e.g. a bank keeping data for 7 years. Lawyers 13 years.

Reasons of public interest in the area of public health

Scientific, historical research or public interest archiving purposes

For supporting legal claims.

The construction & energy law specialists

The GDPR Right to Erasure...reality check

FENWICK ELLIOTT

Not Going to Happen

Some personal data sets are impossible (or **infeasible**) to edit to remove individual records, e.g. a server backup or a piece of microfiche. Whilst these uneditable data sets are in-scope of the erasure Right, themselves they would be out-of-scope for erasure editing procedures due to their immutable nature. If you can destroy the whole microfiche and not worry about losing other data then great. It's the "editing" of microfiche that wouldn't be possible here.

The Real World

Once an organisation understands where all a subject's personal data resides, an assessment must be made of what can be, should be, can't be, and is infeasible to be erased. The exceptions above will commonly apply, such as legal requirements for data retention. But this doesn't mean that the controller should keep the records "live" in an online system. To best protect the personal data it ideally should be archived away to a more protected and locked down system that meets the retention requirements and also goes as far as possible at meeting the data subject's desire to be erased.

The construction & energy law specialists

The GDPR Right to Erasure...

FENWICK ELLIOTT

My Advice

Erasure is an area where there is no black and white on what must be done. Every organisation, every record and every piece of technology used will require a case by case assessment. For example, some processors provide more granular control of deletion of individual records in cold backups. Some provide none.

The key is to focus on what your rationale would be if you were stood in front of the regulator (e.g. ICO in the UK) or a judge in court. Would you be confident that you had a justifiable position on doing the "right thing" by the data subjects, doing the best you could and had given this enough focus and documented thought? Focus on answering this question and you should be in a solid position.

The construction & energy law specialists

FENWICK ELLIOTT

Key practical points

As long as you can show that you are working towards compliance through the adoption of the relevant tools and processes, the Information Commissioner's Office (ICO) will look favourably on you, in the short to medium term at least.

I say as adjudicators and arbitrators you have a valid lawful basis in order to process personal data!

- For example *the processing is necessary for you to comply with the law (not including contractual obligations*) so HGCRA/LDEDPA/Arbitral Rules appointer, named in Contract etc.

- Or the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

- Or Consent: the individual has given clear consent for you to process their personal data for a specific purpose

Key practical points…

FENWICK ELLIOTT

- You must maintain records on several things such as your processing purposes, data sharing and retention.
- Records must be kept up to date and reflect your current processing activities.
- You may be required to make the records available to the ICO on request.
- Documentation can help you comply with other aspects of the GDPR and improve your data governance.
- Controllers and processors both have documentation obligations.
- For small and medium-sized organisations, documentation requirements are limited to certain types of processing activities.
- Information audits or data-mapping exercises can feed into the documentation of your processing activities.
- Records must be kept in writing.
- Most organisations will benefit from maintaining their records electronically.
- Records must be kept up to date and reflect your current processing activities.

You need a Privacy Notice to say:

FENWICK ELLIOTT

We have reviewed our processing activities and selected the most appropriate lawful bases for our activities.

We have checked that the processing is necessary for the relevant purpose and are satisfied that there is no other reasonable way to achieve that purpose.

We use this privacy policy to document our decision on which lawful bases apply to help us demonstrate compliance with GDPR.

We have included information about both the purposes of the process and the lawful basis for the processing in our privacy notice.

We process personal information on lawful bases and list which of the eight you contend you meet.

FENWICK ELLIOTT

Other strategies

1. Read the GDPR and DPA18
2. Think records
3. There are a number of measures that you can, and in some cases must, take including:

- adopting and implementing data protection policies;
- taking a 'data protection by design and default' approach;
- putting written contracts in place with organisations that process personal data on your behalf;
- maintaining documentation of your processing activities;
- implementing appropriate security measures;
- recording and, where necessary, reporting personal data breaches;
- carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests;
- appointing a data protection officer; and
- 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.

Summary

FENWICK ELLIOTT

1. Some can ignore
2. It will not kill you
3. It may cost you a fortune if you get it wrong
4. Post Brexit it may lose some teeth
5. We will all be watching this space as GDPR, Adjudication and Arbitration is a very small book – currently…!
6. Finally…

The construction & energy law specialists

Santa and GDPR

FENWICK ELLIOTT

There is a joke circulating on the Internet, based on the classic song, “Santa Claus is Comin’ to Town”.

He's making a list.

He's checking it twice.

He's gonna find out who's naughty or nice.

Santa Claus is in contravention of Article 4 of the General Data Protection Regulation.

Ah yes - the cruelty of GDPR – Christmas is cancelled!

FENWICK ELLIOTT

The construction & energy law specialists

Any questions?