Thinking about POPI, a friend or foe?

WERKSMANS
ATTORNEYS

08 October 2020

Not to make you cry

Speakers

Ahmore Burger-Smidt

Director and Head of Data Privacy
aburgersmidt@werksmans.com

Jacques van Wyk

Director of Labour & Employment Practice
JvanWyk@werksmans.com

Neil Kirby

Director and Head of Healthcare & Life Sciences
NKirby@werksmans.com

Tracy-Lee Janse van Rensburg

Director of Banking & Finance
TJvRensburg@werksmans.com

Thin line between love and hate

Consent and Justification

WERKSMANS
ATTORNEYS

Ahmore Burger-Smidt

Director and Head of Data Privacy
aburgersmidt@werksmans.com

Lawful processing

At all stages and times based on at least one legal ground

- Consent
- Contract
- Legal Obligation
- Data Subject Interests
- Public task
- Legitimate interest

LAWFUL - Compliant with laws and legal principles

Appropriate to the nature of the underlying relationship between the responsible party and the data subject

Individuals' rights and the implications of using legitimate interests

Rights for Individuals	Responsible Party's Obligations
Legitimate Interests and the obligation to inform individuals	Responsible Party should be mindful that if Legitimate Interests are used as legal basis for processing, as opposed to other Lawful Bases, data subjects must be told i.e. detail the Legitimate Interests and the right of a Data Subject to object.
Right to erasure and Legitimate Interests	Notwithstanding the instances where a Responsible Party depends on Legitimate Interests for the processing, a Data Subject still has the right to object to the processing of such. It is important to note than although the 'right to erasure' is not a guaranteed right for Data Subject in instances where the processing of Personal Data is founded on Legitimate Interests, this right will apply if a Responsible Party cannot justify the lawfulness of the processing.
Legitimate Interests and the right to object	Where the processing of Personal Information is centered on Legitimate Interests, it is incumbent on a Responsible Party to notify the Data Subjects of their right to object to such processing. A Data Subject may be informed at any point in the data collection process, either at collection of in terms of the Privacy Policy. There may be occasions where a Data Subject's objection to processing may not be sufficient to supersede the Legitimate Interests of a Responsible Party. A balancing exercise must take place in order for Responsible Party to assess the bearing of an individual's objection in order to ascertain how such objection will be dealt with.
Right of data trans border transfer and Legitimate Interests	The processing of Personal Information, on the basis of Legitimate Interests, is not encompassed by the right to transfer.

How legitimate interests might apply

Examples that the GDPR Provides	Explanation
Direct Marketing	Processing for direct marketing purposes under Legitimate Interests is specifically mentioned in the last sentence of Recital 47 of EU GDPR, which reads "The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest"
Reasonable Expectations	The fact that individuals have a reasonable expectation that the Responsible Party will process their Personal Data, will help the make the case for Legitimate Interests to apply when conducting the balancing test
Relevant and Appropriate Relationship	Where there is a relevant and appropriate relationship between the individual and the Responsible Party in situations where the individual is a client or in the service of the organisation. Legitimate Interests is more likely to apply when the processing is less likely to be unexpected or unwanted
Strictly Necessary for Fraud Prevention	This could include verifying that the registered address of the cardholder for a particular credit or debit card is the same as the cardholder's normal place of residence or work
Organisational	Where Responsible Party are part of an group or institutions affiliated to a central body that transmit Personal Data within that group or to the central body
Network & Information Security	Where the processing of Personal Data is strictly necessary and proportionate for the purposes of ensuring network and information security. An example of this would include monitoring authorised users' access to a Responsible Party 's computer network for the purpose of preventing cyber-attacks

Examples of where legitimate interests may apply

Examples (This List Is Not Exhaustive)	Practical Examples
Fraud Prevention	An insurance company wants to process Personal Data as part of its business critical anti-fraud measures. This is clearly in the interests of the Responsible Party but could also be seen as benefiting customers as the cost of fraud is one of the factors that can push up insurance premiums for all
Risk Assessment	Insurance companies need to risk assess potential customers to determine what products or services they can offer and the terms of those services. They also need claims information to prevent and detect fraud. Such an industry database also allows insurers to gather relevant information from across the industry to assess and resolve claims more efficiently, and to prevent and detect fraud
Due Diligence	In addition to carrying out statutory requirements, companies may wish to conduct further and necessary corporate due diligence on customers, potential customers and business partners. As well as providing keyword searches of industry and reputable publications to determine if companies and individuals have been involved in or convicted of relevant offences, such as fraud, bribery and corruption
Individual Rights	A business needs to continue processing Personal Data on an individual who has exercised their right to erasure/to be forgotten. This activity would be in the mutual interests of the individual who wishes their privacy rights to be upheld and the business which is required to fulfil this right
Network Security	As specified in its IT governance policies, a company monitors access to accounts containing Personal Data by named users within the organisation to prevent theft of data by employees. The company regards this as essential processing activity to protect its customers

Case Study and example of where legitimate interests may apply

Telematics

Telematics is the transmission of data around remote devices or vehicles over a network. It is used for a multiplicity of purposes such as:

- Monitoring vehicle performance, driving behaviour and road safety

Telematics performs a variety of roles including:

- Promoting the safety of drivers using the vehicles
- Processing traffic offences and incidents
- Processing location and other data for both safety of the driver as well as protection of third parties in the event of a machine malfunction

Legitimate Interest?

There may be a legitimate interest for businesses to safeguard that vehicles being operated by their employees are being operated in the appropriate way

Legitimate Interest test example

Questions	Answer Using Telematics	Guidance
1. What is the purpose of the processing operation?	To use telematics to track the location of the Controller's vehicle/machine and by association, the driver as a data subject, for the analysis of the performance of the vehicle/machine and of the driver and for the protection of third parties.	The first stage is to identify to a Legitimate Interest – what is the purpose for processing the personal data?
2. Is the processing necessary to meet one or more specific organisational objectives?	Yes The processing is necessary for the business to monitor vehicle performance, driver behaviour and ensure road safety	If the processing operation is required to achieve a lawful business objective, then it is likely to be legitimate for the purposes of this assessment. The focus when answering this question should be on your business objectives not the interests of your consumers.
3. Is the processing necessary to meet one or more specific objectives of any Third Party?	Yes, if the Third Party supplies telematics product for the Controller and hosts the information.	A Third Party is any organisation/individual with whom you may share data for their own purposes. While you may only need to identify one Legitimate Interest for the purposes of a Legitimate Interest Assessment – the interest that you are seeking to rely on - it may be useful to list all apparent interests in the processing, those of you as the Controller, as well as those of any Third Party who are likely to have a Legitimate Interest.
4. Does the GDPR, ePrivacy Regulation or other national legislation specifically identify the processing activity, subject to the completion of a balancing test and positive outcome?	No.	For example: Legitimate Interests might be relied on where an individual's (including client or employee) information is processed by a group of companies for the purposes of administration (Recital 48).
5. Why is the processing activity important to the Controller?	It is important to the Controller for compliance with health and safety legislation, as well as protecting the rights of individuals and for monitoring the performance of employees in accordance with employees' rights. Whilst also ensuring employees comply with the employer's policy in respect of operating vehicles.	A Legitimate Interest may be elective or business critical; however, even if the Controller's interest in processing personal data for a specific purpose is obvious and legitimate, based on the objectives of the Controller, it must be a clearly articulated and communicated to the individual.
6. applicable, why is the processing activity important to Third Parties the data may be disclosed to?	The machine that is driver operated utilises lithium ion batteries which carries certain risks and tracking the location of the machine is important for responding to machine malfunctions amongst other Things	A Legitimate Interest could be trivial or business critical, however, the organisation needs to be able to clearly explain what it is. Some purposes will be compelling and lend greater weight to the positive side of the balance, while others may be ancillary and may have less weight in a balancing test. Consider whether your interests relate to a fundamental right, a public interest or another type of interest. Just because the processing is central to what the organisation does, does not make it legitimate. It is the reason for the processing balanced against the potential impact on an individual's rights that is key. It is important to consider whose Legitimate Interests are being relied on. Understanding this will help inform the context of the processing. In combination with the reason the Personal Data is being processed, this information will determine the weight of the Legitimate Interest that needs to be balanced.

Questions?

From recruitment to dismissal

An employers obligations under POPIA

WERKSMANS
ATTORNEYS

Jacques van Wyk

Director of Labour & Employment Practice
JvanWyk@werksmans.com

Hypothetical Example

ABC is a multinational company with local offices in the Western Cape.

Employees access the office by means of their thumbprint.

ABC's business is the processing of credit information on behalf of customers.

ABC makes use of a company to recruit its employees, Recruitment Pty Ltd.

ABC stores the majority of its information digitally using a cloud based systems, whose servers are located in Norway.

ABC is a 'designated employer' for the purposes of the Employment Equity Act.

Status of Parties

- ABC is a 'responsible party'.
- ABC processes the personal information of its employees and applicants for employment (data subjects)
- ABC must comply with the 8 principles

Other considerations

- Special protection is afforded to 'special personal information'
- Race an ethnic origin' processed for EEA / BBEE purposes
- Trade union information - if necessary to achieve the aims of the trade union

Process with POPIA applied

In the beginning… POPIA applied

- Vacant position advertised - request information necessary for finding the best candidate
- Applicants consent to ABC processing the information
- Make it clear - the employer is the Responsible Party.
- An agency running the recruitment process is the operator. Contractual arrangements must be made between the employer and the agency
- ABC to contract with Recruitment Pty Ltd to ensure that Recruitment Pty Ltd has suitable security measures in place to protect applicants' personal information

Recruitment

- Obtaining information from job seekers is "processing"
- ABC must comply with POPIA / the 8 principles of lawful processing and consider where the personal information is stored
- If abroad then cross-border transfer of information
- Unsuccessful applicants - the information supplied must be kept no longer than required by law

During Employment

- ABC and EEA - race and gender information within the workplace
- ABC and employee biometric information - consent must be obtained in this regard.
- Employees processing client credit information must understand ABC's obligations under POPIA

Termination/Post Termination

- ABC must maintain certain documents for prescribed periods of time (EEA/LRA/EEA etc.).
- A document retention register should be maintained in order to manage this process and comply with POPIA.
- Where an employer wishes to retain additional information / information for a period longer than prescribed consent must be obtained.

Questions?

Dealing with Special Personal Information: The Health Of Others

WERKSMANS
ATTORNEYS

Neil Kirby

Director and Head of Healthcare & Life Sciences
NKirby@werksmans.com

Special Personal Information

Health related information

Section 32 of POPIA

Health or sex life is special personal information – processing prohibited in terms of section 26

Special Personal Information

BUT…

Medical professionals, healthcare institutions/facilities, social services – "proper treatment and care" or administration of the practice

Insurance companies, medical schemes, administrators and MCOs – assessing risk, performance of an agreement, contractual rights and obligations

Schools – special support

Managing the care of a child

A public body managing a prison or detention centre

"Administrative bodies", pension funds, employers or institutions working for them – implementation of laws, support for workers in connection with sickness or incapacity

Special Personal Information

An obligation of

CONFIDENTIALITY

Special Personal Information

Inherited Characteristics (section 32(5) of POPIA)

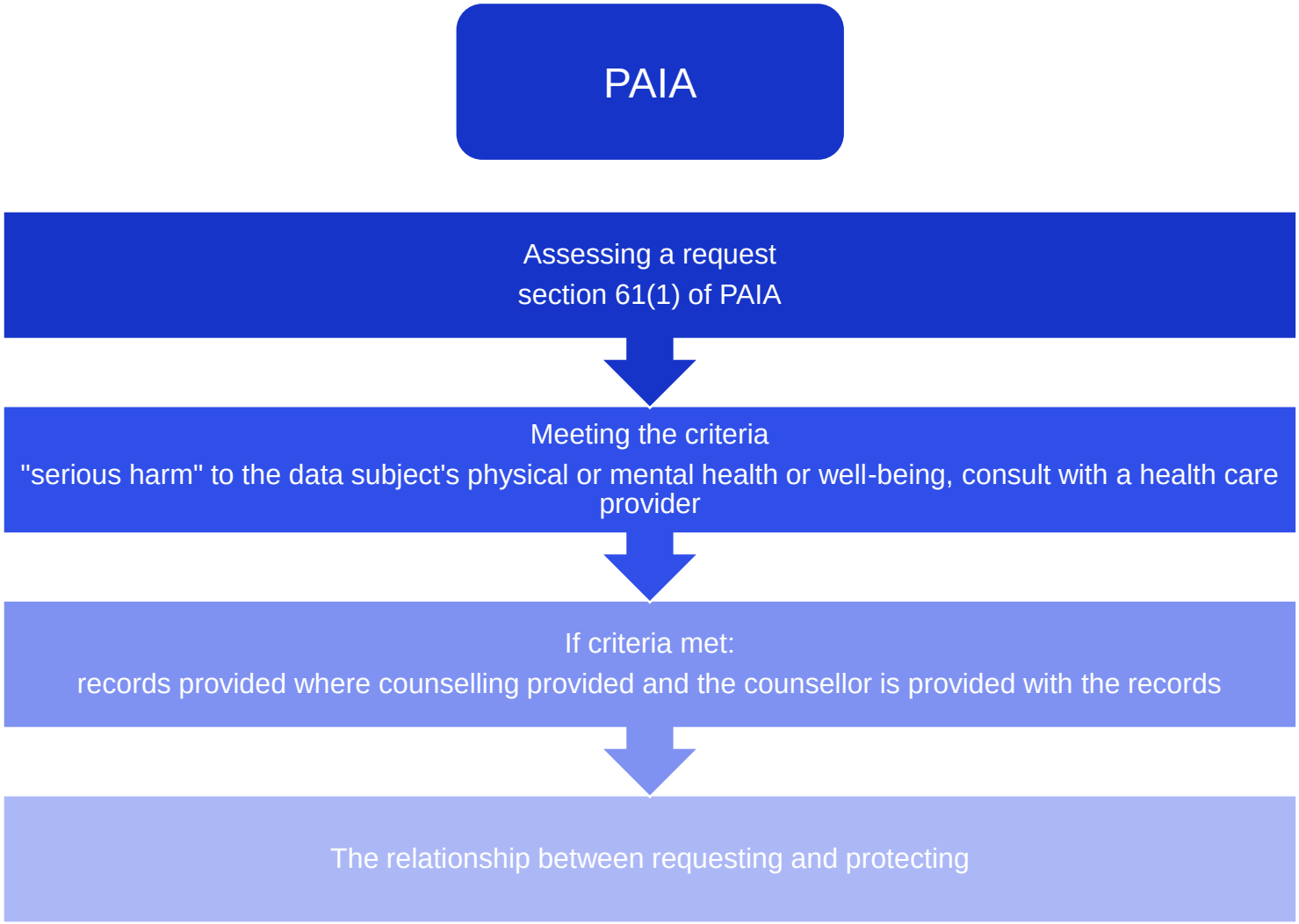
- Overall prohibition
- "serious medical interest prevails" (?)
- Historical, statistical, research activity

Special Personal Information

BEFORE WE GET CARRIED AWAY:
What of PAIA?
(section 25 of POPIA)

- Information available but only through PAIA
- Includes section 32
- The right to request in section 23 – Condition 8
- Sections 31 and 61 of PAIA are applicable to requests

Special Personal Information



Questions?

Security Safeguards and Cybersecurity -

Data Breaches

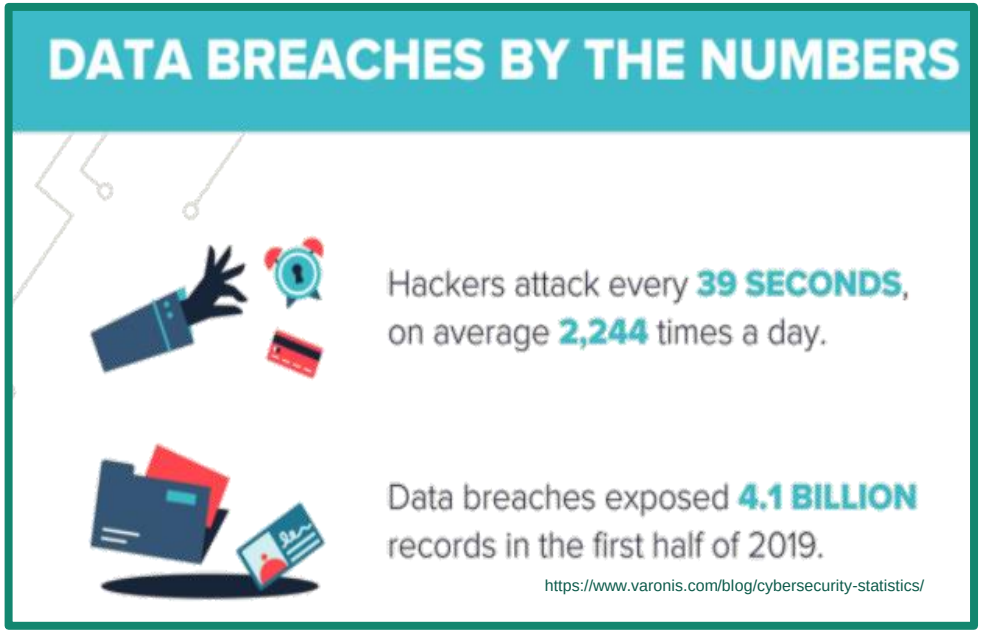
WERKSMANS ATTORNEYS

Tracy-Lee Janse van Rensburg

Director of Banking & Finance
TJvRensburg@werksmans.com

Cybersecurity

- Protect Networks
- Cyberattacks
- Cyberattack Risks
- Plan
- Maintenance



Cybercrimes Bill

Criminalises identified list of "cybercrimes", which includes:

- Unlawful accessing: of data, computer program, computer data storage medium or computer system
- Unlawful interception of data:

  Includes the acquisition, viewing, capturing or copying of data through hardware or software tools
- Unlawful acts in respect of software or hardware tools: the unlawful and intentional use or possession of software and hardware tools used in the commission of a cybercrime
- Unlawful interference with data or computer program: the unlawful and intentional interference with data, computer program, computer data storage medium or computer system

Cybercrimes Bill

Cyber Fraud

- fraud committed by means of data or a computer program or through the interference with data, a computer program, computer data storage medium or computer system

Cyber forgery

- the creation of false data or a false computer program with the intention to defraud

Malicious communications

- distribution of data messages with the intention to incite the causing of damage to property or to incite violence against or to threaten a person or group of persons

Offences

Any person who unlawfully and intentionally commits a cybercrime is guilty of an offence

Any person who conspires with aids, induces, incites, instructs or procures a person to commit a cybercrime is guilty of an offence

Sentences range from 5 to 15 years imprisonment and/or imposition of a fine

Penalties for cyber fraud are very broad and courts can impose a penalty they deem appropriate under section 276 of the Criminal Procedure Act

Obligations for businesses

Businesses, electronic communication service providers and financial institutions have obligations in relation to –

Reporting cybercrimes	Preserving evidence in relation to the commission of a cybercrime

Reports to be made within 72 hours after becoming aware of the offence.

Failure to comply with obligations is an offence, liable on conviction to a fine of R50,000

Obligations for business

Businesses who are victim to a cybercrime or who have an employee who commits a cybercrime must –

Cooperate with and assist law enforcement in their investigations

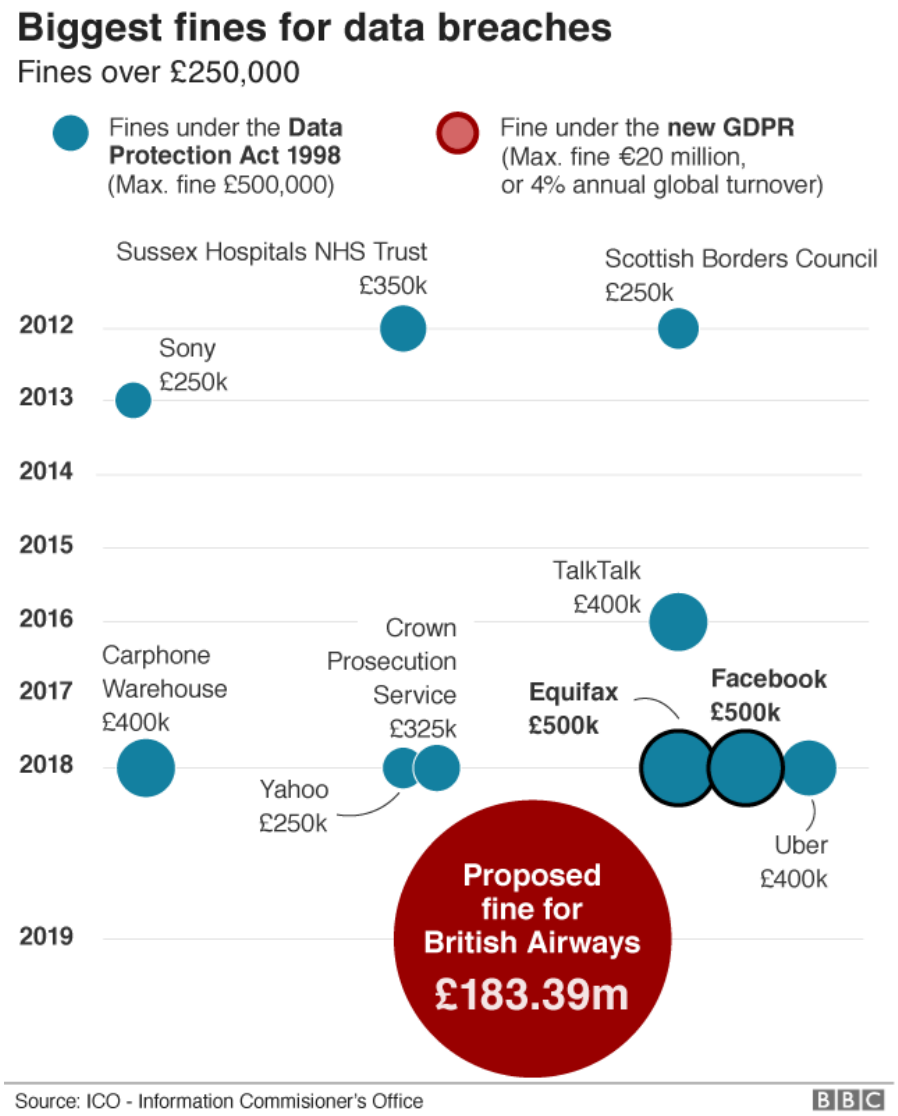
Comply with search warrants

Comply with directions issued by court

Easy Jet

- Data of **9 million customers** affected by a "highly sophisticated cyber attack"
- Email addresses, travel details, credit and debit card details accessed
- Became aware **January 2020,** notified customers (credit cards) in **April 2020**, went public in **May 2020**
- UK Information Commissioners Office ("ICO") notified and investigating
- Under GDPR: EasyJet could face a fine of up to 4% of its annual worldwide turnover or **£17 million** (whichever is higher)
- Facing potential group litigation of up to **£18 billion**

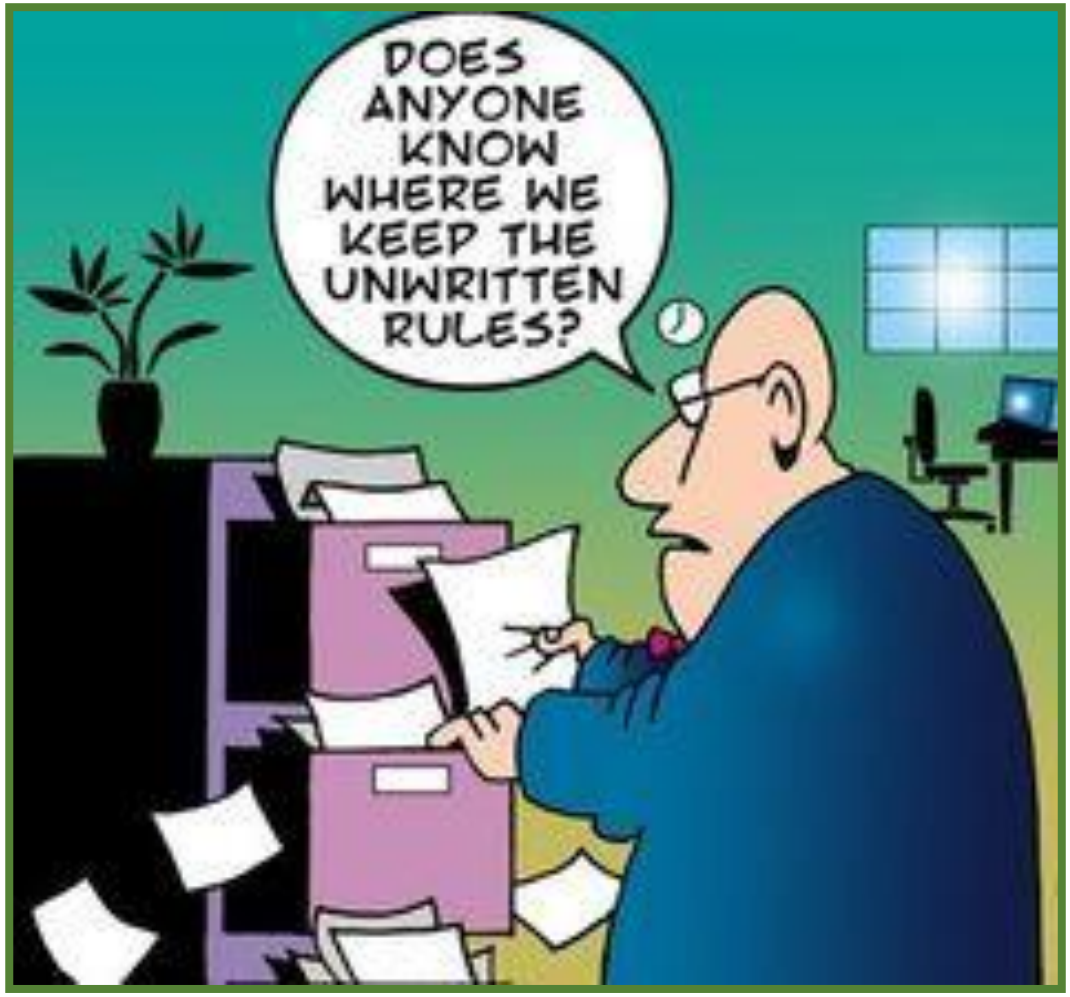
British Airways



- September 2018 personal details of more than half a million customers hacked
- ICO issued £183,39 million fine, together with compensation pay-outs to customers, could see this reach £3 billion

Questions?

Know the rules



Thank You

08 October 2020

Presentation and recording will be made available on request.