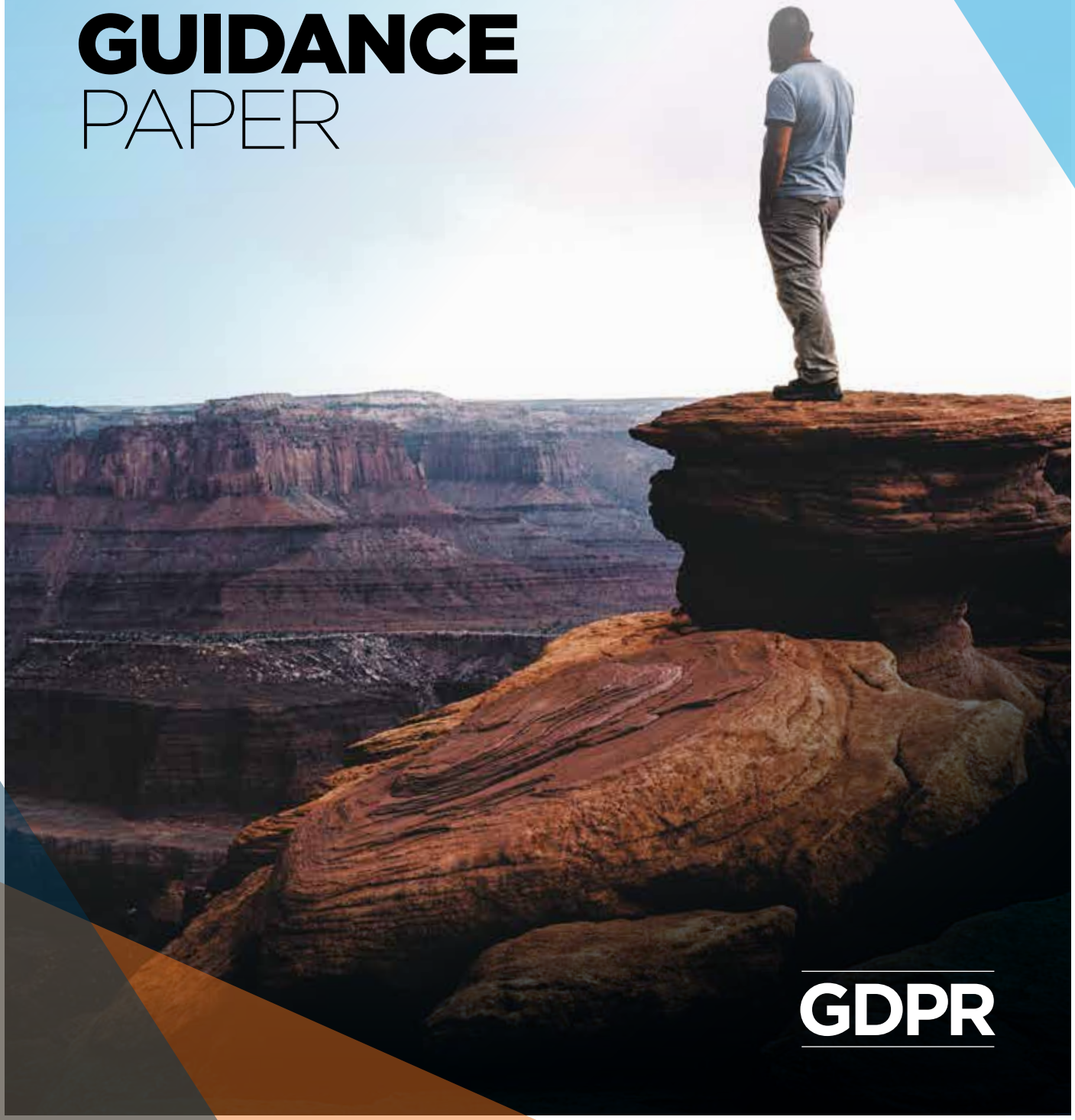
IRM
INFORMATION
RISK MANAGEMENT

DATA PORTABILITY

GUIDANCE PAPER



GDPR

IRMSECURITY.COM

DATA PORTABILITY ARTICLE 20

GDPR AND NEW DATA PROTECTION LAWS BUILD UPON THE RIGHTS OF INDIVIDUALS AND INTRODUCE NEW CONCEPTS SUCH AS DATA PORTABILITY.

These rights are underpinned by provisions for individuals to seek compensation or damages, and even enables consumer groups to take collective actions where these rules and rights are not upheld.

Data portability provides the capability for data subjects to obtain and reuse their data for their own purposes across different services. The rationale for data portability make sense in that if I want to switch bank, utility company, Telephone Company or mobile network I want to be able to do this quickly and seamlessly. However for most Data Controllers and Processors data portability is quite complex and challenging.

There is much uncertainty about regarding the definitions and explanations as to what this really means to organisations and even less idea or understanding amongst organisations themselves as to what they are going to do and more importantly how they are going to do it.

Put simplistically data portability is an extension of an individual's right of access to their personal information, and being able to use those rights in order to collect or obtain the information themselves or to have it transferred for them from one controller or processor to another.

CATEGORIES

CATEGORIES OF DATA TO WHICH PORTABILITY RULES APPLY:

- Firstly the data must have been provided directly by the data subject;
- The requirement only includes personal data that is processed by automated means (does not include paper records);
- The legal basis for processing is based on consent or the necessity to perform a contract to which the data subject is party.

Data portability applies to personal data that the DS knowingly and actively provided (i.e. name, address, contact details), or personal data this is generated or collected by DS activities by their use of the service (IP addresses, type of device, location – if you wear a fitness tracker this could capture the route you have taken even your heart rate!). It is therefore incumbent upon the business to know, and be able to prove exactly how and by what means they came to be in possession of the information.

When providing data to data subject's to 'Port' elsewhere, the information provided must not infringe the rights and freedoms of others; such as joint account holders information; you would need the Consent of both parties. Likewise for loyalty schemes with multiple family or group members. Also does the information being requested include Intellectual Property or Trade Secrets?

Data portability does not automatically trigger the erasure of data from the controllers' systems (provided the controller has defined business justification and retention periods). However those retention periods cannot be used by the controller to delay or refuse to respond to the data subject exercising their rights.

GDPR Article 19 prohibits the Controller form charging a fee to obtain this data unless it can be demonstrated that requests are manifestly unfounded, excessive or repetitive (by the same DS).

IRM
INFORMATION
RISK MANAGEMENT

SIMPLE STEPS TO FOLLOW

STEP **1 -** What personal data is held – what is in scope for Data Portability (categories of data) Meet your legal, regulatory and contractual obligations.

STEP **2 -** any technical constraints for the porting, and subsequent removal or anonymisation of information (does this involve third party processors).

STEP **3 -** ensure systems, processes and documentation are up-to-date, reflect businesses processes and defined requirements. At the forefront of this must be the ability for the controller to ensure they can confirm and identify the data subject beyond all reasonable doubt.

STEP **4 -** Train staff to handle and respond to requests within timeframes (may also involve third party providers). They will need an understanding of what the DS is asking. This will include help desks and customer support centres who may face questions from DS, as well as the people who will handle and process requests, and the technical teams involved in facilitating the provision of information and the possible purge/destruction/ anonymisation of out-of-date / residual data.

STEP **5** - Tell / inform DS of their rights to Data Portability – update privacy notices and provide details relating to data portability. The individual must understand not just that they have the right to data portability but provide details of the personal data that could be provided and how this would be achieved. If there is a 'choice' this must also be clear so that they understand what they are choosing between and can make an informed decision.

CRITERIA TO CONSIDER

- Is this possible or technically feasible to provide data to DS – what format – the requirement is to provide data in a format that allows for the effective re-use of the data
- First priority is to ascertain, verify/validate the ID of the DS (there would be penalties and consequences for sending someone else's data)
- When you provide the DS their copy, can the residual data be deleted from or anonymised within your systems? Anonymised data does not fall within scope of DP / DS (if done properly)
- Data to be provided "without undue delay, but within "one month" – if there are no processes and idea how this is going to work achieving the timeline will be virtually impossible?
- What is the likelihood of you receiving requests? What volume – how do you know, how would you cope with current resources?
- Consider the extent to which information to which data was knowingly and actively provided by the DS –can they access and copy / download this themselves (may need to add functionality to do this – but could be cheaper and easier solution?
- Data transmissions must be secure (encrypted), and need to be authenticated.
- Will your business be the recipient of data being ported by a DS from another controller? What will the processes and requirements for this entail, how quickly would you process and integrate the DS information? What data will you require (Aligned with relevance and not excessive for its purpose in future processing. If you anticipate customers may port data to you, you need to provide clear guidance on what you need/expect from them and the process they need to follow – set expectations and ensure your systems and processes live up to them!
- Data portability can **equally apply to employee data** – giving them the right to port data from one employer to another.

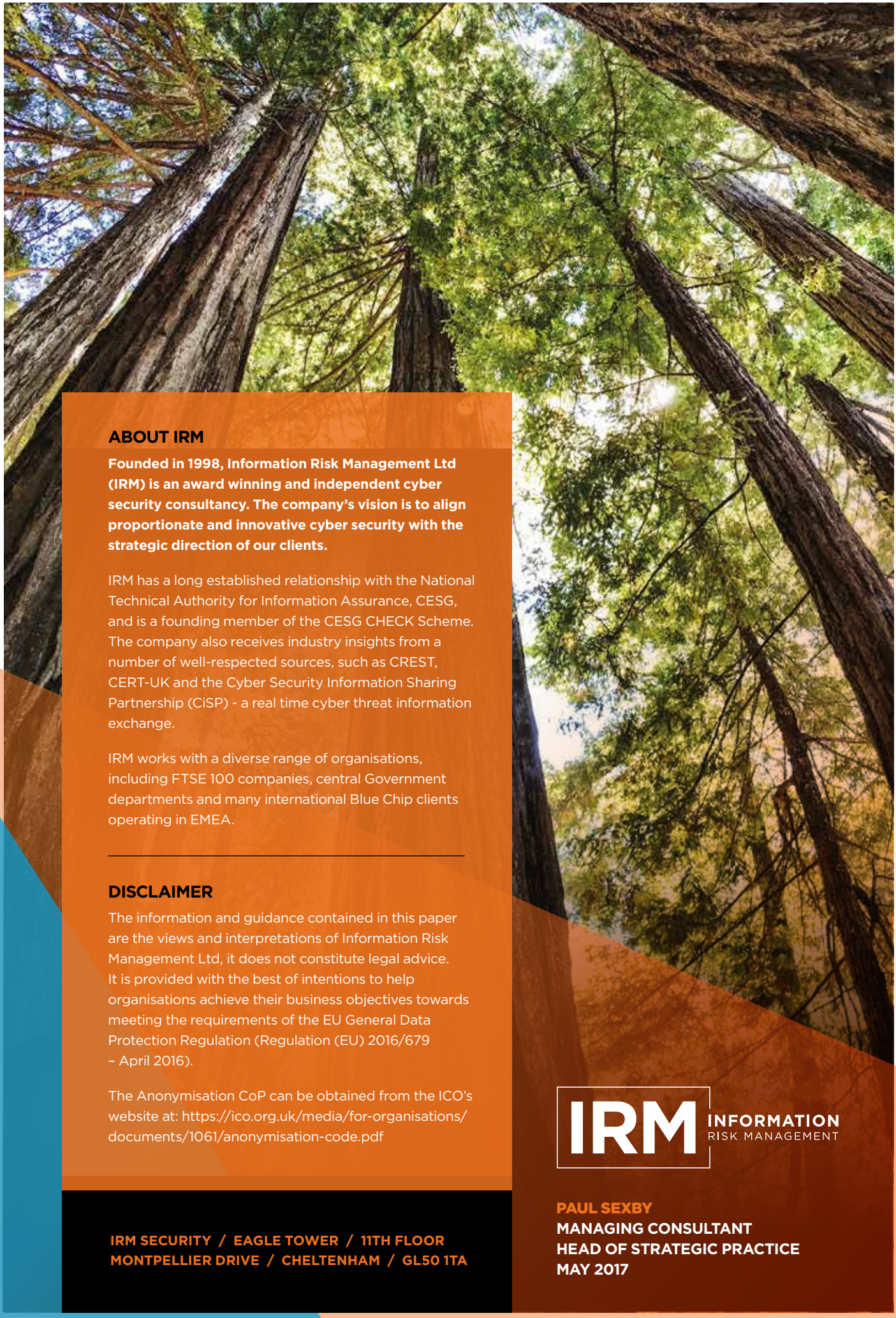
CONCLUSION

In limited situations Data Portability could be a useful right for individuals, as they switch to find the best deals between comparable services. Its use and application in the wider context and situations is unclear.

It is beholden upon organisations to have a plan and associated processes to cover the possibility that someone will ask to port their data!

In some instances building the processes and technologies to support this requirement could require a significant investment. However until you have fully assessed the requirements this is speculation.It may be one of those procedures that is scarcely used, but where you can "pull the file" containing the process it will help ensure you are able to respond appropriately. Conversely, if you do not have a process you could be in a bit of trouble, and are unlikely to be able to respond within defined timelines (i.e. one month), and would suffer the potential consequences that could bring about.

HAVING DEFINED PROCESSES COULD BE A DIFFERENTIATOR – MAXIMISE THE OPPORTUNITY PRESENTED



ABOUT IRM

Founded in 1998, Information Risk Management Ltd (IRM) is an award winning and independent cyber security consultancy. The company's vision is to align proportionate and innovative cyber security with the strategic direction of our clients.

IRM has a long established relationship with the National Technical Authority for Information Assurance, CESG, and is a founding member of the CESG CHECK Scheme. The company also receives industry insights from a number of well-respected sources, such as CREST, CERT-UK and the Cyber Security Information Sharing Partnership (CiSP) - a real time cyber threat information exchange.

IRM works with a diverse range of organisations, including FTSE 100 companies, central Government departments and many international Blue Chip clients operating in EMEA.

DISCLAIMER

The information and guidance contained in this paper are the views and interpretations of Information Risk Management Ltd, it does not constitute legal advice. It is provided with the best of intentions to help organisations achieve their business objectives towards meeting the requirements of the EU General Data Protection Regulation (Regulation (EU) 2016/679 – April 2016).

The Anonymisation CoP can be obtained from the ICO's website at: https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf

IRM INFORMATION RISK MANAGEMENT

PAUL SEXBY
MANAGING CONSULTANT
HEAD OF STRATEGIC PRACTICE
MAY 2017

IRM SECURITY / EAGLE TOWER / 11TH FLOOR
MONTPELLIER DRIVE / CHELTENHAM / GL50 1TA