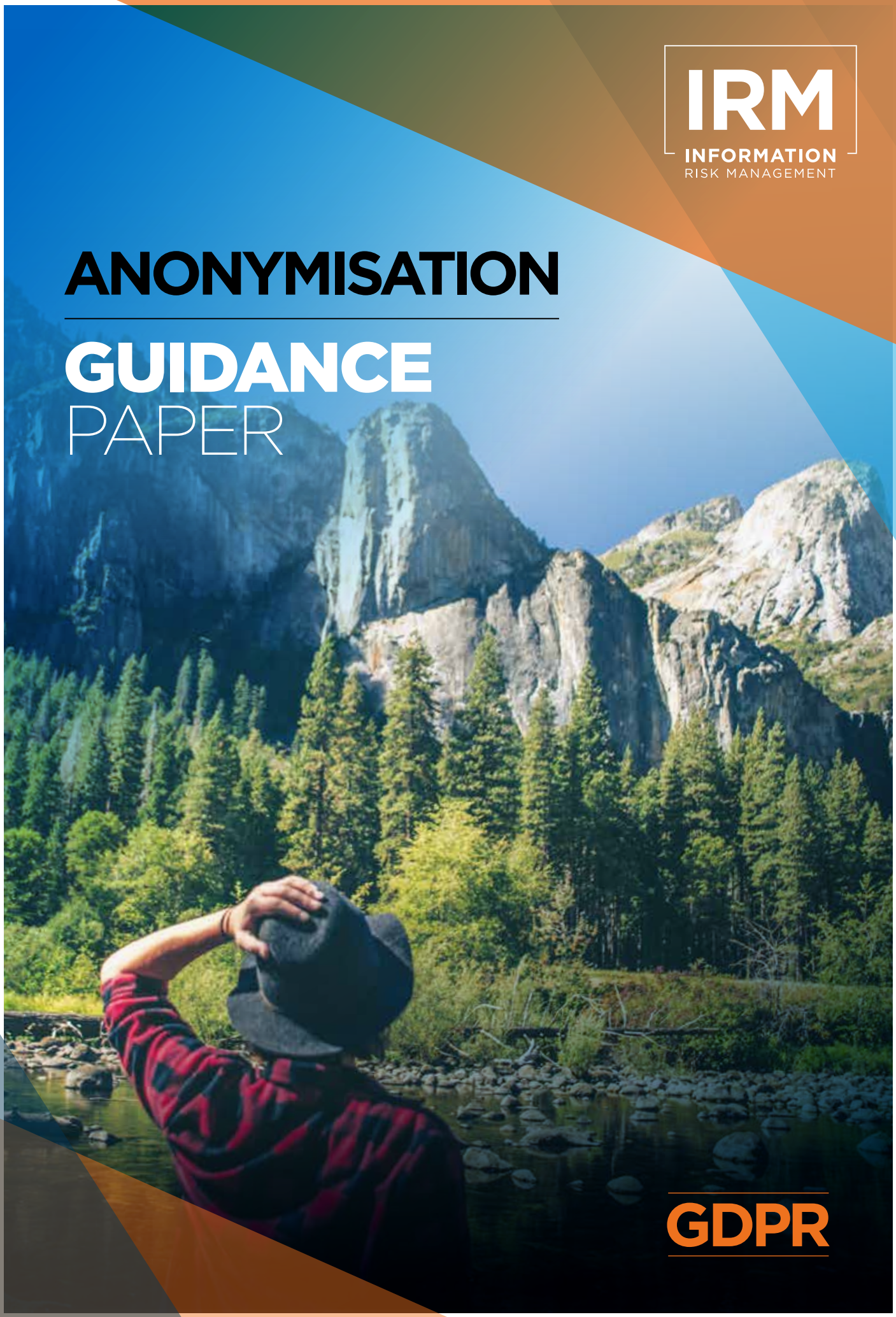
IRM
INFORMATION
RISK MANAGEMENT

ANONYMISATION

GUIDANCE
PAPER



GDPR

IRMSECURITY.COM

INTRODUCTION

ANONYMISATION IS THE PROCESS OF TURNING (PERSONAL DATA) INTO A FORM WHICH DOES NOT IDENTIFY INDIVIDUALS AND WHERE SUBSEQUENT IDENTIFICATION IS UNLIKELY TO TAKE PLACE.

Anonymisation can be a valuable tool in the business armoury as one means of helping to ensure the continued availability of data resources for business needs whilst protecting individual's personal data. Importantly anonymisation reduces compliance obligations and overheads towards current Data Protection legislation and the impending EU General Data Protection Regulations (GDPR). Data protection law and regulations do not apply to data that has been rendered anonymous.

CODE OF PRACTICE

In November 2012 the UK Information Commissioner's Office (ICO) published a Code-of-Practice (CoP) which is still extant today, explaining the data protection implications of anonymising personal data.

Adopting the recommendations in the CoP will help the anonymisation of personal data so that an individuals' privacy is not compromised by an inappropriate disclosure through re-identification.

ADVANTAGES OF USING ANONYMISED DATA INCLUDE:

- Protection against inappropriate disclosure of personal data;
- Fewer legal restrictions apply to anonymised data;
- Anonymised data may be used in new and different ways because legitimate purpose limitation rules do not apply;
- The disclosure of anonymised data is not a disclosure of personal data even where the data controller holds the key to allow re-identification to take place.

Organisations must ensure they have effective governance structures in place to manage and regularly review their anonymisation processes in order to identify any weaknesses or breakdowns in that could cause the data to fall back under data protection governance rules.

It is therefore essential that a thorough privacy impact assessment (PIA) is conducted to determine the likelihood and potential consequences of re-identification and disclosure of anonymised data. The PIA will also need to consider factors such as:

- Will the resulting information still reasonably likely allow an individual to be identified?
- The likelihood of re-identification being attempted and if it could be successful
- Is the resulting anonymised information fit-for-purpose for which it is intended?

The risk of re-identification differs according to the way in which anonymised information is disclosed, shared or published:

- Publication is potentially more risky than restricting and controlling access;
- Limited access allows the disclosure of 'richer data', but relies on more robust governance controls pertaining to its use.

IRM
INFORMATION
RISK MANAGEMENT

The consequences of re-identification of anonymised data could be significant, because it would subsequently expose data subjects to the risks associated with damage, distress or financial loss of their personal information.

ORGANISATIONS SHOULD:

- Seek the data subject's consent for the disclosure and explain its possible consequences;
- Adopt a more rigorous form of risk analysis and anonymisation; or
- Only disclose to a properly constituted closed community with specific safeguards in place.

Spatial information e.g. post-codes, GPS data and map references constitutes personal data. There is no simple rule for handling this kind of data. A simple guide though is to consider the use of Area Codes rather than full post-codes; Area codes cease to fall under data protection regulations.

Similarly dates of birth contain the date/month/year. If this can be reduced to the month/year – it no longer requires to be retained under data protection rules. The date of birth can use used to perpetrate identify theft/fraud; the impacts to individuals can be very significant if this is misused.

Data protection rules in themselves do not prevent organisations disclosing anonymised information, however there may be other reasons for withholding such data. Nor is it always necessary to seek the data subjects' consent to anonymise personal data, one of the other processing conditions should provide a viable alternative. Provided that there is no likelihood of the anonymisation causing unwarranted damage or distress to individuals and you satisfy another condition there is no need to obtain consent as a means of legitimising the processing.

When disclosing anonymised data, consideration must be given to whether disclosures are compatible with individual rights provided under the European Convention on Human Rights and other relevant statutory prohibitions.

Organisations who anonymise data are advised to undertake testing to identify if other data can be discovered and linked to the anonymised data that would result in the re-identification of the data subject. Using penetration testing techniques:

- Attempt to identify individuals and private attributes relative to them;
- Employ methods and techniques and obtain any lawful data source which is reasonably likely to be used to identify individuals within the data set.

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).

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

01242 225 200 HELLO@IRMSECURITY.COM IRMSECURITY @IRMSECURITY