# TREATMENT OF PAPER AND BACKUP TAPES UNDER THE GDPR

CAMERON ALEXANDER
CONSULTANT, IRON MOUNTAIN PROFESSIONAL SERVICES

GARY RYLANDER
MANAGING DIRECTOR, IRON MOUNTAIN PROFESSIONAL SERVICES

The upcoming May 2018 EU General Data Protection Regulation (GDPR) presents organizations with a number of challenges regarding data privacy and information governance in general. The GDPR extends the scope of the EU data protection law to all foreign companies processing data of EU residents. In particular, the GDPR will help safeguard data subject's personally identifiable information (PII) – i.e. information that can be used on its or together with other information to determine a person's identity, locate an individual, or contact a particular person (including information that is unique to a person or that can de-anonymize anonymous personal data).

The key goal of the GDPR is to harmonize EU data protection regulations – impacting companies established in the EU or doing business with an entity in that region. If you are resident in an EU member state, hold data on EU residents or want to do business in the EU then you must comply. Failure to comply with the GDPR's requirements can result in severe penalties of up to 4% of annual global turnover or €20 Million (whichever is greater).

Given the severity of noncompliance, organizations need to be able to effectively respond to data subject requests – identifying the PII at issue, locating where that information exists within its database(s), and editing/updating that information accordingly. Amongst the latest concerns presented by this regulation are two key questions:

# ARE PAPER RECORDS WITH PERSONAL DATA COVERED UNDER THE GDPR AND IF SO, UNDER WHAT CONDITIONS?

## CONCLUSION

Paper records with personal data are covered under the GDPR for any organization that is processing personal data and has a filing system in place that structures personal data according to specific criteria relating to individuals whether centralized, decentralized or dispersed on a functional or geographic basis.

## DISCUSSION:

The actual text of the GDPR does not make any specific reference to either medium of personal data, paper or electronic. However, certain provisions of the GDPR identify paper records in such a way that indicates paper records do fall within its scope. Under the right to data portability of Article 12(5), a data subject may transmit his/her personal data to another data controller – either by the data subject receiving a copy of the personal data and giving it to the new controller, or by having the first controller transfer the data to the new controller. This right empowers the data subject to have more control over his/her personal data, but that right is not infinite – the right does not apply to paper records. Rather, it only applies to data processed by automated means – personal data which the individual provided to the controller, and the basis for processing is consent based on a legitimate interest of the employer or to fulfill specific obligation (such as payment of taxes or terms of an existing contract).[18] The fact that the GDPR's right to data portability carves out an exception for paper records supports the notion that the GDPR is, at the very least, cognizant of paper.[19]

One should also consider that the entire purpose of the GDPR is to control the way personal data is handled and how it is protected. To fall within the purview of the GDPR, personal data has to be "processed".[20] As noted by the UK Bar Council, this has a very broad reach - encompassing the collection to storage of personal data, adaptations and alterations, consultation and use, all the way through to its destruction.[21] And that is not limited to just electronic processing methods – it includes hardcopy (i.e. paper) files as well. However, those hardcopy files need to be part of a filing system in order to be considered "processed".[22]

As set out in the GDPR, a filing system is defined as "[a} structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographic basis". This runs very similar to the EU Data Protection Directive (95/46/EC)'s approach which stated that there is only a right of access to personal data in manual files that is "structured" according to specific criteria relating to individuals allowing easy access to the personal data.[23] The 1998 Data Protection Act had indicated that information held

18 http://www.cicm.com/wp-content/uploads/2017/07/CSA-GDPR-guidance-Jan-17.pdf

19 The GDPR's awareness of paper records is supported the Article 29 Working Party's past guidance on personal data, which stated: "...the concept of personal data includes information available in whatever form, be it alphabetical, numerical, graphical, photographical, or acoustic...It includes information kept on paper, as well as information stored in a computer memory by means of binary code, or on a videotape, for instance. This is a logical consequence of covering automatic processing of personal data within its scope."

https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/int/20070710_harmonisering_speerpunt_wp136.pdf

20 https://www.barcouncil.org.uk/media/619455/it_panel_gdpr_blog_update_the_players_on_the_data_protection_stage.pdf

21 Id.

22 Id.

23 http://www.5rb.com/wp-content/uploads/2013/10/Durant-v-Financial-Services-Authority-CA-8-Dec-2003.pdf

on manual files is only capable of being personal data if it forms part of a system structured by reference(s) to information about an individual as to make that information readily accessible.[24] That said, case law has interpreted the scope of what constitutes a filing system more narrowly. In Durant vs. Financial Services Authority, the English Court of Appeal described a "relevant filing system" as one in one in which the files forming it are structured or referenced in such a way that clearly indicates at the outset if personal data is held within that system, for which files it is held, and has mechanisms in place indicating whether and where such files can be located. [25]

The key term to focus in on here is the word "structured". If the personal data is scattered across different files, then it is not structured and does not fall within the definition of a filing system. For example, a filing cabinet containing HR records arranged in alphabetical order by employee name(s) would be considered a filing system - whereas an unstructured box of hardcopy case files arranged by year with no other labels or identifying info would not. Those hardcopy files would, as a result, fall outside the scope of the EU data protection law(s) until the underlying data gets structured or processed for some other purpose.[26] The fact that there is no other further discussion or treatment of processing paper versus electronic records does not, by omission, exclude paper records from the GDPR's scope. And until case law or supervisory authority says otherwise, this means that the GDPR obligations apply equally to paper as well as digital content.[27]

Several industry experts and business leaders also believe that the GDPR does, in fact, apply to paper records. Jonathan Armstrong of Cordery, co-author of 'Managing Risk: Technology & Communications' and one of the most influential figures on data security in Europe, has stated that paper records are clearly included within the purview of the GDPR. Organizations are still dealing with an immense volume of physical files – many of which exist in disorganized and unsecured fashion on desktops and around offices.[28] And considering that roughly one in every five data breaches that occurs is due to physical files, Armstrong believes that those paper documents are surely covered by the GDPR in exactly the same way as digital files.[29] That opinion is shared by other industry leaders such as Xenith Document Systems' managing director Justin Milligan, who has stated that the GDPR applies on a far wider scope to manually filed paper than the old Data Protection Act ever did.[30]

The opinions of Armstrong and Milligan should also be read in the context of growing data security concerns. The UK's data protection regulator, the Information Commissioner's Office (ICO), indicated that 40% of data security incidents recorded between July and September 2016 were attributable to paper.[31] A 2014 PwC report, in conjunction with Iron Mountain – which surveyed European mid-market companies about how they perceive and manage their information risk – found that two-thirds of respondents said that managing the risks associated with paper records was a top concern.[32] However, research by analyst group Quo Circa stated that only 38% of UK organizations' GDPR strategy included paper, versus nearly 75% of US multinationals' GDPR plans encompassing printed records.[33] Further troubling are numbers put forth by Iron Mountain's own research – which shows that close to a quarter (22%) of companies have no policy regarding paper filing and allow employees to decide what to do for themselves.[34] This data emphasizes not only the relevancy of paper records in the GDPR era, but also the implications of not taking the appropriate measures to ensure that personal data is handled in an appropriate manner.

24 Id.

25 http://www.5rb.com/wp-content/uploads/2013/10/Durant-v-Financial-Services-Authority-CA-8-Dec-2003.pdf

26 https://www.whitecase.com/publications/article/chapter-3-subject-matter-and-scope-unlocking-eu-general-data-protection

27 Additional guidance may come from the independent European Data Protection Supervisor (EDPS), which is set to replace the Article 29 Working Party. The EDPS will consist of its own Supervisor along with senior representatives from the national Data Protection Authorities (DPAs). The EDPB's will be responsible for issuing opinions and guidance – helping ensure consistent application of the GDPR and reporting to the European Commission. https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/64--guide-to-the-gdpr--european-data-protection-board.pdf?la=en

28 https://www.independent.ie/business/world/firms-urged-to-protect-hard-copy-data-35626271.html

29 Id.

30 https://www.computing.co.uk/ctg/news/3017248/gdpr-organisations-ignoring-paper-based-risks-warns-xenith-md-justin-milligan

31 https://ico.org.uk/action-weve-taken/data-security-incident-trends

32 https://www.commerce-associe.fr/wp-content/uploads/files/documents_FCA/Beyond%20good%20intentions.pdf

33 https://www.computing.co.uk/ctg/news/3017248/gdpr-organisations-ignoring-paper-based-risks-warns-xenith-md-justin-milligan

34 http://www.continuitycentral.com/index.php/news/erm-news/833-paper-records-represent-a-significant-general-data-protection-regulation-compliance-risk

# ARE BACKUP TAPES COVERED UNDER THE GDPR?

## CONCLUSION

While not specifically mentioned in the regulatory text, backup tapes are likely within the purview of the GDPR. Past guidance and recent legislation specifically calls out backup tapes as a recognized storage format – with the GDPR most directly impacting the timeliness and defensibility of identifying personal data stored with those formats.

## DISCUSSION

At present, an estimated 45-49% of organizations are still using backup tapes. There's nothing wrong with this – it involves low cost and scale making it the default choice companies utilize as part of their backup and recovery strategy.[18] In discussing the GDPR, some experts have posed that those regulations do not apply since backup tapes aren't specifically mentioned in the regulatory text itself. However, this perspective is a bit misguided in two important ways.

First, let's consider the "omission in the text" argument. While it is true that the term "backup tapes" is not explicitly mentioned in the text of the GDPR, Article 4 of the GDPR specifically discusses processing of personal data by means of collection, storage, or retrieval.[19] Backup data (kept via onsite and offsite storage) would, by all accounts, fall under that definition.

According to chatter on industry forums, some members have received guidance from EU data commissioners informing them that backup tapes fall within the purview of the GDPR, but at this point there is no 'official' guidance.[20] In discussing the definition(s) of personal data, the Data Protection Commissioner of Ireland has stated that backup systems are an essential means of recovering from the loss or destruction of data, with the frequency and nature of that backup depending on, amongst other factors, the type of organization and nature of the data being processed.[21] Furthermore, the pre-GDPR definitions of personal data have been viewed in broad terms and deemed technology neutral - it does not matter how personal data is stored (on paper, on an IT system, on a CCTV system, etc.).[22] The Spanish Data Protection Agency (one of the toughest data protection authorities in the EU) has even gone so far as to require that organizations have a security document on file that outlines the procedures for backup and recovery of data processed or contained in automated filing systems.[23]

Recent legislative enactments further hammer this point home. In Germany, the recently enacted Data Protection Amendment Act (GPDAA) aims to align with the upcoming GDPR. In outlining the data subject's right to access, the GDPAA specifically recognizes that certain data may be stored to comply with statutory retention provisions, or for the purposes of data backup or data protection control.[24]

Yet another issue arises when considering how organizations are able to retrieve specific target files containing personal data from within those

18 http://www.computerweekly.com/podcast/Tape-backup-vs-disk-backup

19 Article 4 of the GDPR defines processing as: "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction" http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

20 https://forums.veeam.com/veeam-backup-replication-f2/general-data-protection-regulation-gdpr-t40950.html#p238244

21 https://www.dataprotection.ie/docs/Data-security-guidance/1091.htm#14

22 https://www.dataprotection.ie/docs/What-is-Personal-Data/210.htm

23 https://www.hldataprotection.com/files/2015/07/Hogan-Lovells-Data_Protection_In_Spain-2015.pdf

24 https://www.twobirds.com/en/news/articles/2017/germany/germany-is-the-first-eu-member-state-to-enact-new-data-protection-act-to-align-with-the-gdpr

same backup tapes. Data backup tapes' legitimate, intended purpose is to facilitate recovery during a disaster recovery window.[25] Outside of that window, or unless on a legal hold, there is no valid operational purpose for maintaining it.[26]

However, Article 17 of the GDPR establishes a "right to be forgotten" – where an individual can request that a data controller erase his/her personal data without undue delay.[27] The GDPR also shortens response time for processing such requests (a copy of the information must be provided in one month instead of 40 days), and organizations can only recoup a "reasonable fee" if the request is manifestly unfounded or excessive due to its repetitive character.[28] In the backup tape context, responding to such a data subject's request would require organizations to identify specific target files with those imaged tapes, and then go through a process of selective deletion and reimaging in order to remove the personal data at issue. Even if the GDPR's permissible extension of two months is deemed necessary[29], this raises a concern as to whether as to whether it is technically correct to apply the GDPR's right to erasure to personal data found on backup tapes.[30] An organization could maintain its databases "in a form which permits identification of data subjects for no longer than is necessary", but drilling down into the backup tapes storing that data may prove time-consuming and costly – a legitimate concern given the risks of non-compliance.[31]

Some organizations may attempt to circumvent this issue by restoring the backup via native software or using any of a number of third party products commonly used to extract responsive backup content for eDiscovery purposes, which can offer a greater degree of precision and accuracy in identifying the target files (and personal data found therein). However, unlike the Federal Rules of Civil Procedure which call out backup tapes as being 'unavailable' and require a higher burden to support production of ESI from backup tapes, the GDPR is silent as to the burden of restoring backup tapes to remove information which must be 'forgotten'. Moreover, the use of native software can involve too many moving parts, any number of which might impact the essential capability of the backup tape – to facilitate restoration.

One of the reasons we must face this quandary about how to address backup tapes in the age of the "right to forget" is that in many organizations backup tapes have become a sort of pseudo archive. This has happened even though every records management authority has advised for years against doing do. Iron Mountain Professional Services regularly advises clients not to include backup tapes as part of a records retention schedule and there are many publicly available articles in Iron Mountain's Knowledge Center explaining the difference between an archive and a backup and advising against the use of a tape for backup when that tape is formatted in a proprietary backup format. Tapes make for a marvelous media for high density, low cost archives, but only when formatted using Linear Tape File System (LTFS) where individual files on the tape are indexed in an open directory structure.

25 https://ico.org.uk/for-organisations/guide-to-data-protection/principle-5-retention/

26 https://community.jisc.ac.uk/blogs/regulatory-developments/article/gdpr-backups-archives-and-right-erasure

27 Article 17 of the GDPR defines the "right to be forgotten" as: "the right to obtain from the controller the erasure of personal data concerning him or her without undue delay" http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

28 https://www.itgovernance.eu/blog/en/the-gdpr-how-to-respond-to-subject-access-requests/

29 http://www.allenovery.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf

30 https://www.slaughterandmay.com/media/2536105/what-do-employers-in-the-uk-need-to-know-about-the-general-data-protection-gdpr-from-an-employment-perspective.pdf

31 Article 5 of the GDPR states that "personal data" shall be: "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed" http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

So what can be done to mitigate these concerns? Some public entities (such as the UK Commissioner's Office) have released guidance materials suggesting different steps to be taken to help ensure GDPR compliance.[18] These measures include:

1. Evaluate current risk: Implement tools such as Risk Assessments or Privacy Impact Assessments will help you identify to what degree backup tapes pose a problem to your organization.

2. Update policies and procedures: Ensure that all stakeholders and departments are following the same approach in regards backup tapes with the GDPR.

3. Educate and inform across the company: The threat of non-compliance is significant enough that privacy should be everyone's concern. Designating key personnel (such as a Data Protection Officer) to take on such responsibilities is a critical consideration (and required of certain organizations).

4. Business process and data mapping: Outlining your organization's current business processes will help you identify the scope of your data storage practices. Data mapping efforts can then show what records an organization has, identify where/how that data is stored (including backup tapes), the sensitivity of that information, who has access, and help set the framework for responsiveness to data subject requests in the future.

5. Review data retention policy(s): Implementing a policy-based approach helps organizations profile backup data once it is no longer used for disaster recovery; determine what is required for long-term retention; and migrate that content out of backup and into a policy-based archive. Once this is done, the remaining backup data can be purged.

Looking ahead, many experts are predicting a shift to a "tapeless age" – one where the threat of GDPR noncompliance looms so large that organizations will reduce their reliance on backup tapes. Organizations will increasingly shift to a cloud-based approach - changing specific processes and storage formats to help ensure compliance in the GDPR era. To move along with this shift to a "tapeless age", organizations should also:

- Ensure that backup data (on tapes, disks, or other physical media) is securely stored via up-to-date encryption methods;

- Ensure that target files within backup data are readily accessible to effectively respond to data subject requests;

- Identify third-party vendors that provide more cost-effective means of accessing data within backup tapes; and

- Migrate records across all departments to cloud-based services for future data storage needs.

18 https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

800.899.IRON
IRONMOUNTAIN.COM

WE PROTECT WHAT YOU VALUE MOST™

**ABOUT IRON MOUNTAIN**

Iron Mountain Incorporated (NYSE: IRM), founded in 1951, is the global leader for storage and information management services. Trusted by more than 220,000 organizations around the world, and with a real estate network of more than 85 million square feet across more than 1,400 facilities in over 50 countries, Iron Mountain stores and protects billions of information assets, including critical business information, highly sensitive data, and cultural and historical artifacts. Providing solutions that include secure storage, information management, digital transformation, secure destruction, as well as data centers, art storage and logistics, and cloud services, Iron Mountain helps organizations to lower cost and risk, comply with regulations, recover from disaster, and enable a more digital way of working. Visit www.ironmountain.com for more information.



USDM-WP-040618A