Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Centre for Information Policy Leadership

White Paper

Data Subject Rights under the GDPR in a Global Data Driven and Connected World

8 July 2020

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Table of Contents

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Following the European Data Protection Board's ("EDPB") stakeholders' event in Brussels on November 4th, 2019, on Data Subject Rights ("DSR"),[1] the Centre for Information Policy Leadership (CIPL)[2] submits this White Paper (the "Paper") as input for the EDPB's future guidelines on DSR (the "EDPB Guidelines" or the "Guidelines").

The EDPB's stakeholder event on DSR addressed the following GDPR provisions: the right of access (Article 15), the right to rectification (Article 16), the right to erasure (Article 17), the right to restriction of processing (Article 18) and the right to object (Article 21). This Paper examines how these particular DSR should be applied in today's global data driven and connected world to be effective. It does not directly cover the topics of transparency[3] and the right to portability[4] (unless they are related to the other DSR).

1. Preliminary Comments

CIPL welcomes the EDPB's initiative to include guidelines on DSR under the GDPR in its 2019/2020 work program. Together with the principles in Article 5[5] relating to processing of personal data, including the principle of accountability, DSR are one of the core building blocks for effective protection of personal data.[6] Non-compliance with DSR can potentially give rise to the highest fines under the GDPR, i.e., up to 20 000 000 EUR or up to 4% of the total annual worldwide turnover. As part of their accountability obligations, organisations have invested significantly in technologies, processes, human resources and training[7] to be able to respond to the increase in DSR requests. They have generally been able to answer them satisfactorily. However, some challenges and uncertainties remain with respect to the full extent of

[1] https://edpb.europa.eu/news/news/2019/edpb-stakeholder-event-data-subject-rights_fr

[2] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 90 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

[3] See CIPL Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR 19 May 2017.
https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf

[4] See CIPL's comments on the Article 29 Data Protection Working Party's "Guidelines on the right to data portability" adopted on 13 December 2016.
https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_wp29_data_portability_guidelines_15_february_2017.pdf

[5] Unless otherwise indicated, all references to "Article" or "Articles" refer to GDPR articles.

[6] DSR are also expressly mentioned in Article 8 of the Charter of Fundamental Rights of the European Union: "Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified"
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN

[7] See CIPL report "What Good and Effective Data Privacy Accountability Looks Like: Mapping Organisations' Practices to the CIPL Accountability Framework" page 32. https://www.informationpolicycentre.com/organizational-accountability.html

their obligations and the efforts needed to properly address DSR requests.[8] Yet, the right to protection of personal data is not an absolute right and must be balanced against other fundamental rights.[9] Likewise, DSR should not be understood as unlimited rights and boundaries must be set up by the EDPB and Data Protection Authorities ("DPAs") to strike an appropriate balance between protecting the essence of DSR and enabling a reasonable and proportionate response by organisations. Thus, CIPL recommends that the EDPB take into account the following preliminary considerations:

- **DSR must be interpreted in the context of our data driven economy**: Because organisations' business practices and the role of data in society have evolved significantly since DSR were first introduced by Directive 95/46,[10] any Guidelines should take into account new business models, data-driven processes and, more generally, the new data economy and digitisation of society. This evolution has created a shift in the way DSR should be balanced against other fundamental rights, including the freedom of expression and the freedom to conduct business.

- **DSR must be interpreted, applied and enforced in a harmonised manner**: The lack of harmonisation across the EU in how the DSR are applied may negatively impact their effectiveness.[11] A common interpretation of DSR is key to ensuring that individuals enjoy the same level of protection across the EU and that organizations can more effectively implement their obligations across multiple jurisdictions. Unfortunately, DPAs have issued a plethora of guidelines and standard forms.[12] To drive increased consistency, CIPL recommends that the EDPB take an approach similar to that of the EDBP draft guidelines on the right to be forgotten.[13] These guidelines describe the applicable grounds to exercise DSR and will be supplemented by an appendix dedicated to the assessment of criteria for handling complaints by the DPA (in the event that an organisation refuses to delist). Providing DPAs with a common assessment matrix to handle all DSR requests would enable more consistency in their implementation.

- **DSR must go hand in hand with educational and digital literacy initiatives**: There are perhaps no provisions of the GDPR more in need of guidance than the DSR provisions. They have led to a significant increase in complaints to DPAs,[14] and organisations are faced with growing numbers of ever more complicated DSR requests. Such requests are driven, in part, by the public's lack of

[8] See Contribution from the Multistakeholder Expert Group to the Commission 2020 Evaluation of the GDPR of 17 June 2020 at pages 8 and seq. https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=41708

[9] See Recital (4) of the GDPR. See also blog of the Irish Data Protection Commission https://www.dataprotection.ie/en/news-media/blogs/data-protection-not-absolute-right

[10] See articles 12 to 15 of Directive 95/46/EC of 24 October 1995.

[11] For example, a divergence exists in relation to the volume and scope of the copies of personal data that need to be provided as part of a right of access request.

[12] See CIPL's report on GDPR evaluation at pages 4 and 8 https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_eu_commission_consultation_on_gdpr_evaluation__28_april_2020_.pdf.

[13] Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1). Adopted on 2 December 2019. https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-52019-criteria-right-be-forgotten-search_fr.

[14] Most One-Shop-Shop cases are related to DSR exercise. See https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_en

understanding of data uses and by a variety of GDPR myths.[15] As part of their mission to promote public awareness,[16] DPAs and the EDPB have an important role to play in properly communicating and educating individuals on the purpose and limits of DSR,[17] and communicating that they should not be abused for fishing expeditions against organizations.[18]

- **The DPO should not have front-line and sole responsibility to deal with incoming DSR requests**: As per Article 39, the DPO must assist the organisation in setting up the relevant policies, procedures, trainings and audits to enable the exercise of DSR. Further, an organisation must be able to distribute the responsibility to respond to DSR requests across different teams within the organisation as appropriate (for instance customer relationship department for customers' DSR requests, human resources department for employees and candidates' DSR requests). The DPO may also be a point of escalation in case of complex cases. Finally, while pursuant to Article 38(4) the DPO must address any issues related to the exercise of rights that are directed to him or her by individuals, this does not mean that the DPO is the organisation's primary contact with front-line responsibility for incoming DSR requests. Rather, organisations may set up DSR response mechanisms wherever appropriate within the organization, and the DPO may be involved in their resolution when necessary or when contacted directly by individuals on a relevant issue.

- **Organisations should get credit for setting up effective DSR processes:** These processes generally enable organisations to address the bulk of DSR requests satisfactorily. In exceptional cases leading to enforcement, an effective DSR process illustrating the efforts of the organisation should be taken into account when deciding on the nature of the enforcement action and used as a mitigating factor when setting the amount of any fine. Holding organisations liable and imposing fines without regard to their due diligence and best efforts may discourage investment in accountable practices (especially if organisations are sanctioned in cases where individuals by-pass existing DSR processes).

- **Certifications covering DSR processes must be a mitigating factor in enforcement:** Certifications serve to demonstrate the value that an organisation places on data protection and its accountability to both the ecosystem and individuals. They are based on an independent evaluation of an organisation's compliance with data protection laws. They also provide the highest possible level of assurance with regards to the design, implementation and operating effectiveness of internal controls under an organisation's privacy management program or

[15] See note 8 at page 5 "there are misunderstandings leading to the assumption that it is always necessary to obtain their consent or that the right to erasure is absolute. Dealing with these misconceptions is often time consuming. Several members underline that further work is still required to ensure that individuals understand properly the scope of their data protection rights".
[16] See Article 57(1)(b) of the GDPR.
[17] For example, some individuals have requested that banks delete bad debt or bad fraud history, or universities to erase grades of failure to an exam.
[18] A "fishing expedition" is defined as (1) a legal interrogation or examination to discover information for a later proceeding; or (2) an investigation that does not stick to a stated objective but hopes to uncover incriminating or newsworthy evidence. See Section 2(h) for more examples on DSR requests being used as fishing expeditions.

particular processes, including the handling of DSR requests.[19] Consistent with Article 83(2)(j) and (k),[20] a certification must be considered as a mitigating factor in cases where an individual has a valid DSR complaint and enforcement (including a fine) is being considered by a DPA.

- **The DSR Guidelines should remain principles and risk-based:** Given the variety of potential situations in which DSR may be exercised, it is important that the upcoming Guidelines remain principles and risk-based and not be too prescriptive. The Guidelines should define the outcomes that organisations should seek, leaving it to organisations to define the specific DSR processes that are most effective in their own context. In addition, how DSR may apply in specific situations or sectors may be further specified in instruments such as certifications or codes of conduct.[21]

- **The DSR Guidelines should account for Article 23 of the GDPR:** While the Guidelines' objective is to frame the scope of DSR, they should not interfere with the possibility for member states to restrict DSR in specific limited cases through legislative measures. CIPL underlines, however, that there are several national laws pre-dating the GDPR that already de facto limit DSR. Moreover, new laws do not always include express restrictions on DSR even though they may restrict DSR in practice. The EDPB should confirm that organisations subject to national laws are expected to comply with these laws, inclusive any restrictions on DSR, so long as such restrictions do not exceed what is necessary and proportionate.

- **The DSR Guidelines should articulate a resonableness test for DSR requests and responses**: The majority of individuals are exercising their rights in good faith. However, a small but active number treat DSR as unbounded, thereby overwhelming organizations with requests. Organisations sometimes have to assess whether each piece of data needs to be provided, in what form, how it should be explained and track retention and deletion. These processes can be disruptive to core business practices, and even more so when DSR are exercised recklessly or for nefarious purposes. With a clearer definition of what constitutes an abusive request, organisations could better allocate their resources and prioritise resolution of legitimate requests.

- **The DSR Guidelines should anticipate exceptional circumstances**: The COVID-19 crisis has highlighted the need for a flexible approach to interpreting some data protection provisions in the case of extraordinary circumstances. The Irish Data Protection Commission has acknowledged the significant impact of the crisis on organisations' ability to address DSR requests in a timely manner as organisations may have to divert resources to priority work areas or face reduced capacity for responding to requests, and indicated that it would consider possible mitigating circumstances in this context.[22] CIPL believes that the EDPB should endorse this approach and

[19] See for instance points 7.3.5 to 7.3.10 of ISO/IEC 27701 on Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management https://www.iso.org/standard/71670.html that provide requirements for handling DSR requests.
[20] Article 83(2)(j) is relevant in cases where the organisation benefits from an Article 42 GDPR certification and Article 83(2)(k) for any other certification.
[21] See Article 40(2) of the GDPR on codes of conduct that cites specifically provides for "[…] (f) the exercise of the rights of data subjects".
[22] https://dataprotection.ie/en/news-media/blogs/data-protection-and-covid-19

more generally encourage regulatory forbearance[23] in exceptional situations (such as pandemics, cyber-attacks, etc.) where the law enables such flexibility.

2. General comments applicable to all DSR requests

a. Verification of the identity of individuals

Regardless of the DSR request, robust identification of the individual is paramount not only to enable the organisation to respond properly, but also to avoid disclosing data to an unauthorised third party. Forged or publicly available information obtained from social media or through social engineering could be used to exercise DSR fraudulently. Disclosing data in the context of responding to these DSR requests could qualify as a data breach under Article 4(12) of the GDPR.[24] Article 12(6) of the GDPR takes this into account by providing the controller with a right to request additional information to confirm the identity of the requestor.

To facilitate the exercise of DSR and reduce the risk of fraud, in line with Recital 57 of the GDPR,[25] the EDPB should clarify that if the method for account creation allows for reasonable identification of an individual, by default, the procedures for exercising DSR should be similar. When the organisation provides products or services to individuals online or through mobile applications with an individual account, the identity of a user as the account holder should be confirmed through the same channel and applying the same security measures to reduce the risk of fraudulent requests. This approach also aligns with Recitals 63 and 64 of the GDPR, which provide that individuals should be able to exercise their rights easily and that the controller should use all reasonable measures to verify the identity of the individual, in particular in the context of online services and online identifiers. There should also be alternative means of identification in the event that the individual is locked out of his/her account, where the account can be used by multiple persons at the same time or if the account has been hacked.

For human resources ("HR") related DSR, the EDPB should clarify that, by default, identification should be made using the employee number or copy of the employee's badge and the last physical address on file. For former employees in particular, organisations should be entitled to request an ID if they believe that the employee identification number is not sufficient.

---

[23] See also the ICO reaction to the COVID 19 crisis https://ico.org.uk/media/about-the-ico/policies-and-procedures/2617613/ico-regulatory-approach-during-coronavirus.pdf

[24] "'[P]ersonal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed[.]" See the EUR 9.550.000 fine of the German Federal Commissioner for Data Protection and Freedom of Information (BfDI) on a telecommunications service provider for breaching Article 32 of the GDPR by providing insufficient technical and organizational measures to prevent unauthorized persons from being able to obtain customer information via the customer hotline service by providing a name and date of birth. https://edpb.europa.eu/news/national-news/2019/bfdi-imposes-fines-telecommunications-service-providers_fr

[25] GDPR Recital 57 "Identification should include the digital identification of a data subject, for example through authentication mechanism such as the same credentials, used by the data subject to log-in to the on-line service offered by the data controller."

In the event that individuals disregard the process put in place by the company (for instance, by sending a letter or fax to the organisation), he or she should expect longer processing times, follow up questions for more information to enable identification, and generally more stringent authentication procedures (for instance by requesting an official ID). If the individual refuses to provide additional information and the controller cannot identify the individual as being an account holder, the EDPB should clarify that in this instance in accordance with Article 11(2), DSR should not apply. This should also help accelerate the management of requests coming from individuals with whom the organisation has no relationship.

In addition, CIPL stresses that organisations have invested resources in developing privacy-by-design safeguards like pseudonymisation, which can make the identification of individuals more difficult. In these cases, and particularly where individuals fail to provide additional information on their identity, Article 11(2) should not be narrowly construed so as to require companies to undergo further costly and intensive manual diligence in all cases to try to re-identify individuals to address DSR requests. Otherwise this may have the adverse effect of not incentivising companies to proactively invest in privacy enhancing techniques.

Further, it may not be possible to validate an individual's identity immediately on receipt of a DSR request. In certain cases, it only becomes apparent after gathering copies of the individual's personal data that identification of the data subject would require further validation because, for example, the date of birth on record does not match the date provided in the request. In such cases, a controller may need to revert to the individual for further proof of identity. The EDPB should acknowledge that time extensions to respond to the DSR requests are applicable in such cases.

The EDPB should also allow more flexibility to respond to a DSR request in the event of a data breach, where organisations may be experiencing a surge of requests after notifying potentially impacted individuals. Organisations may still be investigating the causes and impact of the breach at the time they receive the DSR request and may want to apply specific enhanced identification measures to mitigate possible adverse effects of the breach and prevent fraudsters from taking advantage of the situation. This leniency should apply under strict guidelines for the duration of the investigation of the breach, and organisations should have the opportunity to extend the delay to respond to DSR requests and to apply stronger identification techniques.

Finally, the EDPB should clarify that individuals should first review companies' DSR policies and comply with them, as this is the most secure and effective manner to identify themselves and exercise their DSR. Thus, before investigating a complaint alleging that an organisation has not complied with a DSR request, DPAs should first ensure that the complainant has followed the company's authentication processes. This clarification would also prevent cases where organisations' DSR processes are being tested by individuals sending huge numbers of requests, deliberately ignoring the companies' policies and procedures.

Summary of CIPL recommendations:

- Clarify that procedures similar to account creation should apply in the context of authenticating individuals for the purposes of exercising DSR;

- Consider identification of individuals in relation to Article 11(2) and provide a balanced approach that does not discourage implementation of privacy preserving techniques;
- Consider unusual situations such as incident or crisis management that may justify use of enhanced identification techniques; and
- Clarify that DPAs should verify that individuals have followed a company's identification processes before reviewing DSR-related complaints.

b. Third party exercising DSR on behalf of individuals

Several websites offer individuals the service of exercising their DSR on their behalf.[26] The GDPR requires facilitation of DSR,[27] but it does not specifically address this situation. CIPL would welcome the EDPB's view on how to best address scenarios involving third party services and individuals with whom controllers have no existing relationship. Some organisations report a huge number of requests (+50%) where the requests are entirely speculative. It also appears that the third party industry is "over-processing" personal data on an industrial scale. As a consequence, the EDPB should clarify the approach to the emerging third party DSR industry, including steps to encourage privacy by design and default in the sector.[28]

CIPL underlines that it is very challenging for controllers to verify the identity of users that are represented by a third party. This requires firstly verifying the identity of the third party, and secondly verifying the authorisation given by the individual to the third party, which is generally not given according to an official or standard template. These requests may also come from a no-reply e-mail address that make it impossible for the controller to ask further questions. They are also often not specific about the region where the individual is located, the material scope of the request or the nature of the relationship between the individual and the organisation. CIPL highlights that there is currently no effective way to verify the identity of the individual or the legitimacy of the third party request. As a consequence, this situation actually hinders the ability of controllers to effectively and timely verify the identity of individuals and enhances the risk of committing a possible data breach as the whole construct can serve as an easy conduit for malicious data extractions by cybercriminals who leverage email account credentials, which are available on the dark web by the tens of millions. What can appear on its face as a legitimate request may in fact be a phishing request.

Sometimes, the controller is also required to click on a link and fill out a form at the request of the third party. The extent of the obligation on the controller to log into an external platform to respond to these requests needs to be clarified.

In addition, some third parties make multiple DSR requests (regarding access or portability) on behalf of individuals with their consent, to further process the data of such individuals in ways that may not be fully

[26] See for instance https://justdeleteme.xyz; https://weredavid.com; https://www.fairmi.fr/accueil.php; https://www.deseat.me, https://saymine.com/ or https://www.mydatadoneright.eu/
[27] See Article 12(2) of the GDPR.
[28] Example of best practices could include, for instance, sending messages from the individual's email account or complying with the organisations' designated online procedure to process DSR requests. https://saymine.com/faq#for-companies

compliant with the GDPR. Organisations are forced by current law to hand this data over where the consent is valid, without the usual due diligence that would be carried out if providing information to a supplier acting on the instruction of the controller or to another organisation for a mutual purpose. There is also a risk that third parties abuse the personal data when they receive it on behalf of individuals. In any case, the third party should not be deemed to be acting on behalf of the controller when providing information back to the individual as this would place liability on the controller for potential data misuse where the controller never actually "engaged" the third party in the first place (and no Article 28 processing agreement has been entered into). The EDPB should clarify that in this instance, the controller transferring the personal data should not be responsible for any potential further use (or misuse) of the data.

The EDPB should provide that even if requests are made by third parties on behalf of individuals, controllers should be permitted to not recognise or accept such requests as long as they provide so explicitly in their public privacy notices and policies. In the event that controllers agree to respond to DSR requests submitted by third parties, responses should go only directly to individuals who can then pass data back to these third parties at their own discretion.

Summary of CIPL recommendations:

- Clarify how best to address scenarios involving third party services exercising DSR on behalf of individuals;
- Specify that controllers are not under an obligation to accept third party DSR requests if they so provide in their public privacy notices and policies;
- Clarify that if requests are made by third parties on behalf of individuals, responses should go only directly to individuals; and
- Confirm that a controller transferring personal data to a third party in the context of complying with a DSR request shall not bear any liability.

c. Use of a DSR request tool provided by the controller

In line with their accountability obligations, organisations have spent significant resources on building and acquiring automated tools, have set up entire cross-functional teams (e.g. HR, security, privacy office, legal, engineering, etc.) and trained relevant employees to accelerate DSR request treatment and make their responses more efficient for the benefit of individuals. Some companies have even hired third party service providers to handle DSR requests on their behalf under their instructions.

Consistent with Recital 63 of the GDPR,[29] these tools can be self-service tools that individuals use to download their data (e.g. employees can access an electronic record of all pay stubs at any time). These tools enable access to data and modification and deletion of accounts. They are built to accommodate the most common DSR requests and are set up to cover data that is generally deemed relevant to an

[29] […] Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data […]

individual, based on the services provided or the circumstances of the individual. They generally require individuals to log in, which serves as a means to verify their identity. After the request, individuals receive a confirmation email, and once the data is ready, they get access to a link, which allows them to securely download their data (triggering the access to the data for the individual and the execution of the obligation under Article 15(1) for the controller). When DSR requests are broader than what the self-service tools enable, organisations have put in place specific support teams with different levels of escalation paths to best accommodate these requests.

As a result, when such efforts and investments have been made, individuals should not be automatically authorised to exercise their DSR through other means, especially when the information they request is readily available via the tool. The determination made by the controller that the use of a specific self-service tool, link or identification method is the most secure and effective manner to respond effectively to DSR requests in light of the size or business activity should prevail. Consequently, where requested data is available through self-service mechanisms, controllers should be entitled to refuse to provide bespoke responses outside that mechanism unless the individual can provide specific reasons. Where the individual cannot articulate a valid reason for circumventing the normal process, the controller should not be held liable for not fulfilling the request.

Similarly, if an organisation has taken steps to make information available as part of its day-to-day operations, then it should be able to direct people to this. For example, if an internet banking app allows clients to check if they have a particular product or an HR portal allows employees to see historical performance management reviews, then organisations should be able to direct requestors to these rather than provide them as part of a DSR response. A similar approach is already taken under many Freedom of Information laws[30] and this approach should trigger greater transparency in organisations.

Some organisations believe that there is still room for improvement to facilitate the exercise of DSR and provide user-friendly tools to ensure individuals' identification, or in handling fully automated requests. However, absent a clear acknowledgement that individuals have to use these tools when exercising their DSR, companies may not be incentivized to invest in developing these user-friendly tools.

Summary of CIPL recommendations:

- When a self-service tool is made available by the controller, provide that the controller should be entitled to refuse to provide bespoke responses (and not be held liable for doing so) unless justified by specific circumstances.

d. Time to respond to DSR requests

According to Article 12(3) of the GDPR, the controller shall provide information to the individual on action taken in relation to a DSR request without undue delay and, in any event, within one month of receipt of the request.

[30] A freedom of information (FOI) law allows access by the general public to data held by national governments.

The start date of the one-month period is unclear, as well as the definition of "request." With regard to a vague request that requires additional clarifications or a request that cannot be handled via the self-service tool, the one-month period should not start immediately (see Section 2(e) on addressing unclear requests). This is consistent with Recital 63 of the GDPR, which enables the controller to ask the individual to specify the information or processing activities to which the request relates before data is made accessible. In other words, the one-month delay should only start when (1) the scope of the request is clear and (2) the individual has successfully verified his/her identity. Finally, the same should apply in relation to follow-ups, additional questions, or changes in the scope of the request.

In addition, Article 12(3) provides that the initial one-month period to respond "may be extended by two further months where necessary, taking into account the complexity and number of the requests." The complexity of a request that requires manual extraction or review for the purposes of redacting third party data triggers complex technical processes and may require increased resources in order to gather the personal data (for example a DSR request asking for unstructured data). This should justify an extension. In this situation, organisations may automatically extend the delay to two months by default, or may apply an extension in business days, i.e., 10 to 15 business days.

The definition of complexity requires clarification. Clear EDPB Guidelines would help controllers make more consistent determinations. By itself, volume of retrieved data is not necessarily "complex", however often a large volume equals large volumes of exempt data (third party, proprietary/IP, etc.), especially when the request requires extraction of emails. In addition, CIPL believes that "number of requests" in Article 12(3) should be understood to refer to the following scenarios:

- Significant processing activity relating to one individual generating large amounts of data, or multiple DSR requests by one individual over a short period of time;

- An exceptionally large volume of DSR requests in exceptional situations (such as in case of a data breach, a pandemic or similar situations) and over a short period of time (a spike). For example, a news article about a credit reference agency losing data can increase DSR requests by over 100%. It would be impossible to handle these types of spikes within the prescribed timelines. The same may happen when a new privacy policy is launched (e.g. the changes in privacy policies resulting from the GDPR's entry into force, which generated a thousand deletion requests for one organisation);

- An exceptionally large number of issues are raised or triggered by an access request.

The EDPB should also clarify the computation method of the one-month delay to provide information: if the delay elapses on a bank holiday, the organisation should be entitled to respond by the next weekday.[31] Similarly, in case of national holidays or other office closure days, when offices are closed for a period of time, or national holidays, organisations should be entitled to extend the delay to respond.

In cases where DSR are exercised outside of the organisation processes or a request is sent to the wrong recipient, it should be acceptable for controllers to direct the individual to the appropriate self-service DSR tool where proper authentication measures are in place, and requests can be logged and tracked. In

[31] https://ico.org.uk/your-data-matters/time-limits-for-responding-to-data-protection-rights-requests/

such cases, the deadline for responding to the DSR request should only start once the proper DSR request is made through the DSR request tool.

Summary of CIPL recommendations:

- The one-month delay should not start running until the scope of the request is clear and the requestor's identity has been successfully verified in line with the organisation processes;
- The number of requests that justify an extension should also apply in unusual circumstances where the same controller faces a significant and unusually high volume of DSR requests; and
- The notion of "complex request" should be further clarified.

e. Open and unclear requests

Organisations have received very unspecific and open-ended requests such as: *"you have to erase my data", "this is my right", "my data does not belong to you"* or *"please erase everything*". In some cases, the individual refuses to answer the controller's request for further specification. In these situations, individuals should be required to specify the specific rights they are exercising (right to access, modification, deletion, etc.) as these rights are different and can have different consequences. In addition, CIPL would welcome the EDPB's confirmation that the organisation can address these DSR requests as follows:

- Provide a scoping outline and confirm that it will respond accordingly to the DSR request. In this case, the organisation should be allowed to make its own reasonable and proportionate assessment of the type of personal data that falls within the scope of the request; or,
- Refuse to act on the request on the basis that the DSR request is manifestly unfounded or unclear (see Section 2(h) below).

In some instances, individuals insist on getting access to data that they incorrectly assume exists or is processed in the form they think. In this situation, the individual may end up complaining that the data is not provided in a certain way. This could be the case, for example, when multiple files are provided and when conclusions can be drawn only by combining the files, but the controller does not, in fact, engage in processing of the data involving such combining. If the controller were to respond the DSR request in the manner requested by the individual, this would constitute additional processing, and would go beyond the mere exercise of DSR.

Finally, in cases where the individual exercises his or her DSR with the wrong organisation, such organisation should not be required to direct the individual to the relevant organisation. This is particularly important when a request is addressed to a processor instead of the controller and the circumstances make it impossible for the processor to determine which organisation is actually the controller. This happens typically in multitenant cloud environments, where the request, legally meant for one of several thousands of possible client organisations (themselves being either controller or processor), is submitted to the cloud provider instead. In such cases, not only is the processor legally not the right entity to

respond, but it is also not in a position to figure out who the right entity would be, and can neither advise the data subject, nor forward the request to the client. Indeed, trying to direct the individual to the right client would force the processor to violate the confidentiality agreement with its client, which would not be acceptable. As a consequence, complaints by individuals against processors who have declined to respond to such requests should be dismissed.

The situation would be different only in the case of joint-controllership where – depending on the arrangement between the joint-controllers[32] - the individual should be notified that the other joint controller is the contact point to respond to the request.

Summary of CIPL recommendations:

- Require that individuals clearly specify the right they are exercising;
- Confirm that in the case of vague or open-ended DSR requests, organisations can respond on the basis of their own scoping and assessment or consider the request as unfounded or excessive;
- Confirm that organisations are not required to perform additional processing to respond to DSR requests; and
- Confirm that processors are not required to identify and direct the individual to the right organisation.

f. Scope of data covered

In order to enable organizations to address DSR requests most effectively, CIPL recommends the Guidelines take a reasonable approach in relation to the material scope of DSR. There should be further analysis and thinking as to the relevance of providing all data relating to an individual, in particular as it relates to data created by technologies (e.g., unique ID numbers used by specific internal systems with no meaning outside of the specific system that uses the number, system data that may be tied to a user account, etc.). In certain cases, this data, whether it is raw, analysed or inferred, may be meaningless to an individual, but the organisation still needs to process it for security or traceability reasons.

CIPL believes that the following categories of data should be excluded from the scope of DSR requests or, if not excluded, should be subject to clear guidelines and limitations:

- Unstructured data that is not part of a filing system and requires an actual processing as defined by the GDPR;
- Data that needs to be re-identified at the backend when the controller has taken technical measures to pseudonymize or otherwise de-identify the data for privacy or security reasons;
- Archived and back-up data;

[32] See Article 26(1) of the GDPR.

- Data meaningless to the individual outside of a specific system that cannot be ported, deleted or restricted;

- Data that is retained only for a very short period of time and deleted before the one-month delay to respond to the DSR request elapses.

- Data to which the individual already has access to (including through a self-service tool) or is publicly available.

Summary of CIPL recommendations:

- Provide that in response to DSR requests organizations must provide only such data that is meaningful to individuals; they are not required to provide data whose identification and provision would impose on the organisation undue burdens, additional bespoke processing operations, or otherwise exceed the purpose of the DSR.

g. Limits to DSR requests

Individuals may exercise their DSR for various reasons and the GDPR does not require that these reasons be disclosed to the organisation. This does not mean, however, that organisations must address DSR to the full satisfaction of individuals as DSR are not absolute rights. The standard applicable to DSR implementation is an objective one and should be weighed against other considerations such as the protection of intellectual property and trade secrets, the protection against fraud and security, the proper identification of the individuals, the protection of third parties' rights, the protection of other fundamental rights or the data management and retention policies of organisations, among others.

For the right of access, Article 15(4) provides, for instance, that the right to obtain a copy "shall not adversely affect the rights and freedoms of others." This means that for each request the controller has to verify that the DSR does not conflict with other rights and interests, including those of the controller. Consistent with Recital 63,[33] the notion of "others" appears to include both legal entities and individuals. For the sake of clarity, CIPL would welcome the EDPB's explicit adoption of this interpretation. In addition, below are concrete examples of limits to DSR that organisations have been implementing and that should be confirmed in the EDPB Guidelines:

- **Protecting the rights of third parties** – there are interactions that create personal data, yet the disclosure of such data in the context of a DSR request may lead to a breach of personal data:

  - **In customer/user support interactions**, the name of the employee/agent handling the request, as well as all other personal data relating to this employee/agent, internal notes in

[33] "That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software."

response to a DSR request or recordings of calls between the user and customer support agents;

- **In user bilateral rating systems** where users and service providers can rate each other, the feedback, comments, reviews, complaints, or identity of the individual awarding the rating. Providing this information in response to a DSR request could trigger possible retaliation. This would also run afoul of the expectation of anonymity of the individual providing the review, as he or she would not necessarily expect this information to be shared with the subject of their rating. Moreover, not maintaining an expectation of privacy for such reviews would have a chilling effect and result in fewer and/or less honest reviews;

- **In the recruiting context**, the HR department's interviews of candidates and notes about the candidate, name and notes of the HR employee providing the review;

- **In the employment context**, performance or peer reviews, interview notes, emails, where employees provide written feedback on their colleagues. In these cases, responding to these DSR requests would not be in line with the confidentiality expectations of the individual performing the review. Further, it could curtail freedom of expression or relevance of such reviews if reviewers were warned at the outset that their input could be disclosed to the reviewee. In addition, getting the consent of the third party would not be possible as consent is generally not valid in the employment context. The only way to respond to these requests would be to delete the reviewer's name and any other identification criteria before disclosing the data, but this may not always be possible as the feedback itself may allow for the indirect identification of the reviewer;

- **Respecting Attorney-Client privilege.** It is important to note that the scope, extent, nature and sanction of legal privilege varies from one country to another;

- **Protecting intellectual property, trade secrets and confidentiality.** For example, Article 15(h) which requires providing information about the logic or reasoning behind automated decisions and profiling, could compromise commercially sensitive information without appropriate protections;

- **Protecting against fraud and security.** Disclosing certain personal data to individuals (such as internal identifiers) may have security implications for the organisation as they could be used to game the security system and potentially affect the security of the entire processing. Therefore, responding to DSR requests should not lead to the disclosure of information that would enable the circumvention of security and fraud prevention measures and endanger the protection of personal data of other individuals, as well as the security of the organisation as a whole;

- **Protecting information which another person or party has an overriding legitimate interest to maintain without modification or erasure,** such as employment records maintained to show the employees are eligible for rehire; information necessary to assert or defend against a legal claim, project files, collaboration threads, meeting minutes, comments in documents,

recordings of calls, email threads, records of transactions that have taken place, logs of IT policy and data incidents;

- **Protecting any information if its release, deletion or modification would prejudice** the prevention or detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of any tax or duty or of any imposition of a similar nature;

- **Protecting information relating to on-going negotiations between the organisation and the individual**, where disclosure could prejudice such negotiations;

- **Not deleting information legally required to be retained by the controller** in the event a deletion request;

- **Protecting management information, confidential references, exam scripts and marks**;

- **Applying other exemptions provided for under Member State law as per Article 23 of the GDPR** when necessary to protect other interests, including the protection of judicial independence and judicial proceedings, the enforcement of civil law claims, national security, crime prevention, regulatory functions, etc;

- **Facing technical constraints**: Many organisations have invested heavily in technology, but even state of the art technology (and certainly legacy technology) does not always enable a full search on every imaginable data point. In addition, companies do not generally have a global database where they can search for a name, but instead have several databases covering several regions and processing activities. While outdated technology or decentralised systems should not be a blanket reason to refuse to address a DSR request, the EDPB should recognize that this could be part of the equation when addressing a DSR request;

Summary of CIPL recommendations:

- Recognise that DSR requests can be limited by other compelling interests of the organisation, third parties or society, and confirm a list of limits to DSR requests.

h. Unfounded or excessive/abusive requests

Article 12(5) allows the possibility for controllers to charge a fee or refuse to act "where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character". The EDPB should clarify when requests are manifestly unfounded, excessive, or repetitive by providing clear use cases.[34] This would help controllers understand when they can refuse to act on a request and better allocate resources. Similarly, the EDPB should confirm that DSR requests made within a particular number of days/weeks/months of the last one are abusive. Some organisations consider that repeated

[34] See note 8 at page 11.

requests in a short time, for instance more than 3 requests a month, or even more than once in less than 6 months, are abusive.

In some instances, DSR requests are literally weaponized collectively[35] for unrelated purposes and/or with the sole purpose of disturbing business operations, clogging systems and creating costs for the organisation on the premise that organisations will face potentially huge financial penalties if they do not address the DSR request satisfactorily.[36]

DSR requests can also be weaponised individually to secure data and evidence to enter into legal proceedings against the controller or to add costs or burden to organizations during disputes. Individuals may use DSR requests to seek to encourage a balanced resolution in the context of employment or customer dispute, negotiations preceding termination of employment, a grievance process or litigation. In this situation, DSR requests act as a form of phishing exercise at the request of an individual or are used as a tactic to delay, obstruct or derail business initiatives (such as re-organisations, M&As, divestitures, etc.). This is a complete misuse of DSR that are intended to be a means to verify the lawfulness of processing.[37] For instance, a Dutch Court decided that there was an abuse of rights because the individual filed an access request only to use this information in another legal procedure and not to check the lawfulness of the processing of data.[38]

Other examples of abusive cases in the DSR context include:

- Requests that refer to all data processed about an individual in any form without mentioning the context in which the data is processed;
- Requests covering a huge period of time, for instance a long-term employee asking for copies of all documents in his/her entire professional file for the last 30 years;
- Requests for decades of phone log data from an employee who has worked in multiple different offices globally that would require 15 months of work from one full-time employee;
- Request to receive an entire copy of a file that the individual has lost;
- Requests to search for personal data in unstructured electronic information systems or in back-up tapes.[39]
- Requests that refuse the self-service applications/portals and insist on receiving a copy of the data by post/e-mail;

[35] https://boingboing.net/2019/10/08/ddos-gdpr.html
[36] See note 8 at page 9.
[37] See Recital 63 of the GDPR.
[38] Noord-Nederland Court 23 April 2019, ECLI:NL:RBNNE:2019:3761
https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBNNE:2019:3761
[39] See note 8 at page 11.

- Requests to access all copies of CCTV footage (as well as conference call recordings, meeting minutes, etc.); and

- Requests from employees to receive all emails in which the individual is a sender, recipient, copied or mentioned.

With regard to emails, requests may be particularly problematic as most emails need case-by-case review, since they may include personal data of others or confidential information and require extensive and costly redaction. The process of looking through these emails is not scalable as the redaction cannot be automated and leads to the use of disproportionate efforts for the company responding to such DSR. For this reason CIPL believes that companies should not generally be expected to search and provide all emails that an employee has been included in. Just because an employee is the sender, recipient, mentioned or copied on an e-mail, this does not mean that the email or its content constitutes the personal data of the employee, as the email is not about the employee but rather is about actions and decisions of the legal entity employing him or her. If the relevant correspondence is (i) not about the employee, (ii) not being used to evaluate or treat the employee in a particular way, or (iii) not likely to have an effect on the employee's rights and interests, such correspondence is not employee personal data.

CIPL underlines that organisations generally have been trying to respond to all requests to the best of their abilities without differentiating their responses based on the intentions of the individuals. CIPL believes, however, that because the motivations of some individuals are nefarious and inconsistent with the purpose of DSR, the EDPB should set clear limits to such abuses, which may unnecessarily monopolize company resources that would be better allocated in responding to legitimate DSR requests.

Summary of CIPL recommendations:

- Clarify what constitutes an unfounded or abusive request and set clear boundaries to abusive and excessive requests to enable more efficient DSR implementation;

- Condemn the intentional weaponisation of DSR requests to disrupt an organisation; and

- Clarify that companies should not generally be expected to search and provide all emails that an employee has been involved in.

i. Application of a proportionality test in responding to DSR requests

Proportionality is a general principle of EU law[40] that must inform the scope of a controller's response to a DSR request. In cases where the right to data protection runs up against other fundamental rights, the CJEU has held that it is necessary to strike a "fair balance" between the various competing interests.[41] In

[40] See Joined Cases C-27/00 and C-122/00) R (Omega Air Ltd) v Secretary of State for the Environment Transport and the Regions [2002] ECR I-2569 at [62]
[41] See C-70/10 Scarlet Extended v. SABAM [2011] ECR I-11959.

other words, DSR do not require the imposition of an "excessive burden" on the data controller.[42] For example, in assessing the data that is to be produced in response to a DSR request, controllers should be able to consider whether or not the data is in a retrievable form (e.g. offline log-level information stored in a data warehouse, as opposed to online personal data that is stored on an individual level), and consider the resources and the costs incurred by the controller in retrieving certain information.

The GDPR already requires that costs of implementation incurred by the controller (or processor) be taken into account in several instances: when implementing a request for deletion where the controller has made the personal data public, such controller can take into account the "available technology and the cost of implementation" to inform other controllers processing the personal data that the data subject has requested the erasure of any links to, or copy or replication of, those personal data.[43] The controller must also take into account the cost of implementation when implementing appropriate technical and organisational measures as part of the data protection-by-design-and-by-default principles.[44] Similarly, the controller and the processor shall take into account the cost of implementation of the technical and organisational measures to ensure a level of security appropriate to the risk of the processing.[45] It would not be consistent if organisations were entitled on the one hand to take cost into account when defining privacy-by-design or security measures for processing activities while on the other hand having to bear unlimited costs to respond to DSR requests. All are equally important to process data responsibly and protect individuals' fundamental rights and freedoms.

In a recent judgment of 20 June 2019, the Amsterdam District Court emphasized that it is important for the individual to sufficiently specify a subject access request if the controller processes a large amount of data. The Court decided that a controller can request a specification of the request if the search for the personal data is too extensive for the controller and therefore too expensive. If a search is too expensive, the controller may refuse to cooperate with a subject access request.[46]

In a case of DSR request in the context of an ongoing employment dispute with Oxford University where the University had reviewed 500,000 documents at a cost of £116,116, the UK Court of Appeals noted that the obligation to comply with a DSR request is only an obligation to conduct a reasonable and proportionate search and not "an obligation to leave no stone unturned."[47] A company responding to a DSR request has satisfied its obligations provided that it has conducted a reasonable and proportionate

[42] See C-553/07 Rijkeboer [2009] ECR 1-3889, paragraph 59. When engaging in this balancing exercise, the court will seek to strike fair balance between "on the one hand, the interest of the data subject in protecting his privacy, in particular through his right to have the data communicated to him or her in an intelligible form, so that he is able, if necessary, to exercise his rights to rectification, erasure and blocking of the data (in the event that the processing of the data does not comply with the directive) and his rights to object and to bring legal proceedings and, on the other, the burden which the obligation to communicate such data represents for the controller"(See C-486/12X.at 28.)
[43] See Article 17(2) of the GDPR and right to erasure.
[44] See Article 25(1) of the GDPR.
[45] See Article 32(1) of the GDPR.
[46] Amsterdam Court 20 June 2019, ECLI:NL:RBAMS:2019:4418
https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2019:4418
[47] Ittihadieh v 5-11 Cheyne Gardens, and Deer v Oxford University [2017] EWCA Civ 121,
http://www.bailii.org/ew/cases/EWCA/Civ/2017/121.html

search, even if there is a possibility that additional relevant personal data might still be found if a more extensive search were conducted.

Summary of CIPL recommendations:

- Allow controllers to apply a proportionality test when responding to DSR request; and
- Clarify that cost can be taken into account as a factor in responding to DSR requests and in deciding which DSR requests, or which of a request's aspects are manifestly excessive.

3. Specific comments by type of DSR

a. Right of access (Article 15)

Article 15 provides that individuals have the right to access their personal data and a list of eight categories of information that must be provided, which mirrors the list of information to be provided by the controller under Articles 13 and 14 as part of its transparency obligations. Therefore, for better efficiency and consistency, controllers should be permitted to refer the individual to the privacy notice that is put in place as per Article 12, provided of course that such privacy notice applies to the specific circumstances of the individual. In addition, the controller should be permitted to provide standard information to the individual that he or she can thereafter interpret it in light of the specific situation (i.e. "*if you have used this service or bought a product, this is the type of information we hold about you…*"). Requiring the controller to address each and every case specifically and individually would trigger a huge administrative burden. If the individual makes a second access request based on a specific aspect of the processing, the controller should answer this request in a more granular manner as it relates to the specific individual. This approach, while being more pragmatic and efficient by enabling the individual to get the right information at the right time would not limit the essence of Article 15 to the boundaries of Article 12. This interpretation is confirmed by a decision of the German Hessen DPA regarding "Best Practices on Data Subject Rights" dated 08/16/19[48] which states that, in certain cases, the right to access does not establish an individual right to a copy [of their data], provided a well-structured summary about the processing would satisfy the requirements of Articles 12 and 15. Such summary would provide information about the processing in a precise, transparent and easy to understand manner, allow individuals to submit a subsequent request, complaint, claim for damages or to lodge a complaint with the DPA, and would minimize the risk of disclosing a third party's information while addressing the access request.

Recital 63 of the GDPR states "where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specifies the information or processing activities to which the request relates." In some cases, individuals make a broad access request, requesting all their personal data without specification, for example, in terms of what data they are looking for, what categories of data, related to what context, or for which period. For these cases, organisations should be able to adopt a layered approach: in the initial response the controller provides a copy with the most relevant personal data within one month of receipt of the request. If the individual sends a follow-up request for further information and/or data, the

[48] https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2018_47_TB.pdf at page 78.

controller should have an additional month to undertake a more in-depth, robust, and resource-heavy process, which can vary depending on the specifications provided by the individual (subject to the limits to DSR listed in section 2 of this Paper).

In some cases, organisations ask directly in the initial response that the individual provide further specification of the request. Organisations do this as a courtesy, but CIPL does not believe this should be a requirement in all instances. If the individual refuses to specify the access request, the controller should be able to provide a standard answer. The controller should by no means be required to perform an extensive and costly search of its system to locate as much data as possible on the individual. At the same time, asking an individual to specify the access request or to better scope it, should not be seen as an impediment to the right of access, but as a more effective manner to respond to the request.

Finally, the EDPB should clarify that individuals are not entitled to request the original documents on which these data are based as this goes beyond Article 15 of the GDPR.

Summary of CIPL recommendations:

- Authorise the controller to refer first to information available as per Article 12 when responding to access requests;
- Accept a layered approach when responding to access requests for better efficiency; and
- Clarify that individuals can request a copy of their personal data but not originals of the documents.

b. Right to rectification (Article 16)

The EDPB should clearly define the boundaries of this right so that it applies only to truly inaccurate data or data that needs to be updated because the situation of the individual has evolved. This right should not be used to revise the past (for instance, a change of name or marital status should not have a retroactive effect). In addition, controllers should be able to ask individuals for specific evidence that information held is incorrect.

The notion of "accurate/inaccurate" data should be further specified to apply only to facts and not to opinions. This is also key to protect freedom of expression. The EDPB should clarify that rectification must only apply to inaccurate data and not data that the individual does not agree with, e.g. in employment disputes regarding performance, a 'poor performance' rating for an employee does not warrant a rectification if the elployee disagrees. There are usually other ways to address this such as through HR processes.

Finally, Article 16 is unclear about who bears the burden to verify the accuracy of data and there may be cases where the accuracy/inaccuracy of the data is disputed by the controller. Further guidance from the EDPB or case studies on how far controllers are expected to go to verify accuracy would be welcome.

Summary of CIPL recommendations:

- Specify clear boundaries to the right to rectification so that it does not amount to a right to rectify the past;
- Clarify that the notion of accuracy should not interfere with the freedom of expression; and
- Clarify how data accuracy should be verified.

c. Right to deletion/erasure (Article 17)

The exercise of right to deletion or erasure could have serious consequences for individuals that may not always be in a position to foresee possible short and long-term consequences. To address this, some organisations are taking precautions to ensure individuals understand the consequences of their request by responding with a description of the data that will be deleted and asking for their confirmation so that the organisation may proceed with the deletion, to ensure that nothing is deleted in error. CIPL would welcome confirmation from the EDPB that this is an acceptable approach.

Consistent with the comments already made in section 2 of this Paper, individuals tend to mistakenly believe that erasure is an absolute and unconditional right that applies to all records that an organisation may hold on them. Clearer recognition of the exceptions to the right to deletion through concrete guidance would give controllers more ability to respond to ill-framed or controversial requests and avoid contentious disputes around sweeping erasure requests.

The EDPB should also elaborate further on examples and scenarios where data can be retained after deletion requests, in particular for the purpose of fraud prevention. Some types of fraud are not evident until months after a transaction has occurred. Similarly, organisations would welcome guidance on whether retaining details of customer support interactions (in accordance with a company's standard document retention policy) may be permitted for certain purposes even after an erasure request was made. For example, such retention may be necessary to evidence prior requests, effectively support future requests, or avoid repetitive requests from the same individual.

In addition, some controllers are subject to additional sectoral regulations which require customers' personal data to be kept for a strictly defined period of time, e.g., financial institutions are required to keep data for archiving purposes in connection with anti-money laundering regulations. In practice, this means that a request for deletion cannot be met immediately due to mandatory retention periods. However, controllers frequently encounter pushback from individuals and additional complaints are raised on deletion requests not being addressed properly.

It would be beneficial to continue educating individuals on the valid grounds to request erasure of personal data and cases in which requests may be denied. For instance, in a recruitment scenario, where the candidate ends up not being hired and requests his/her data to be immediately deleted – this request may not be immediately met as internal processes (that translate legal and regulatory obligations) require data to be kept for a certain period of time.

Further, organisations may have to invest significant resources to effectively implement this right as all data that is in the scope of the request first has to be assessed against legal requirements to retain the data. Organisations may also have to create specific systems and processes that work in a particular way (e.g., require account closure at the same time as data deletion) and these systems and processes may not permit amendment for each individual deletion request. As a consequence, the EDPB should acknowledge that the effective implementation of the right to deletion may require more time.

Finally, in cases of requests for deletion in marketing contexts, companies may include a marketing suppression message in the response, such as "*we have deleted your data in accordance with our process, however, your email address will be maintained on our suppression list to prevent you from receiving future marketing messages*." This can trigger a reaction, as it indicates that the organisation has not deleted all the data, but the intention is to honour the essence of the request and to protect the individual with the lowest level of discomfort possible. A "master forget list" must be maintained, otherwise the controller cannot mitigate the risk of unknowingly re-ingesting the data of someone deleted in the past. CIPL would welcome confirmation from the EDPB that this is an acceptable approach.

Summary of CIPL recommendations:

- Confirm that a two-step approach requesting confirmation before personal data is permanently deleted is an acceptable approach;
- Reinforce that the right to deletion is not absolute;
- Acknowledge that sectoral laws may prevent the immediate implementation of a deletion request; and
- Confirm that maintaining an email address on a suppression list in the context of requests for deletion may be necessary.

d. Right to restriction (Article 18)

It appears that individuals have seldom exercised their right to restriction of processing. This may be because its rationale and interaction with other rights are not well understood by individuals and organisations. The purpose, scope and implementation of this right need to be better explained. Organisations also face a number of unresolved issues in relation to this right, such as:

- Whether the data needs to be copied and "preserved" in a database separate from the one where it is normally stored;
- How companies can "restrict" data in systems integrated to services – for instance, how can certain data be restricted in a customer account (like time of last log-in) if the customer then uses the account again subsequent to the restriction;

- Whether it is acceptable to close the account of the individual if the processing of that same data is actually needed to provide the service;

- Which right should prevail in the event that the individual makes a subsequent request of erasure of data with respect to which processing is already fully or partially restricted.

Summary of CIPL recommendations:

➢ Further clarify the rationale and limits of the right to restriction as well as its interaction with other DSR.

e. Right to object (Article 21)

Except in the context of direct marketing, individuals have not widely exercised their right to object so far. This DSR can be exercised when the processing is based on the legitimate interests of the controller or of a third party. There are several pending questions on the consequences and limits of the right to object and the relationship with other DSR. Unanswered questions include:

- If an individual objects to analytics being processed based on his/her service usage, is it acceptable to stop providing the service?

- What does first communication mean in Article 21(4), which requires that the individual be informed of their right to object "at the latest at the time of the first communication"? Would the mention of the right to object in the organisations' privacy policy be sufficient?

- Are there any differences in the practical consequences of the exercise of a right to object and the withdrawal of consent?

Finally, Article 21(1) provides that when an individual objects to processing, the controller shall no longer process the personal data unless it demonstrates compelling legitimate grounds for the processing that would override the rights of the individuals. This requires carrying out a balancing test between the reasons relating to the individual's particular situation and the compelling legitimate grounds for the processing. Consistent with Article 6(1)(f) of the GDPR, the compelling legitimate interests should cover not only those of the data controller, but also those of third parties. Moreover, in cases where the objection is with respect to processing that is based on legitimate interest, it would be helpful to clarify how the balancing test described in Article 21(1) would be different from the initial balancing test performed by the organisation when it relied on the legitimate interest ground in the first place.

In addition, as provided by the EDPB in its draft guidelines on the right to be forgotten, the exercise of the right to object is one of the six grounds for the right to obtain erasure under Article 17(1)(c) of the GDPR. Data controllers have an obligation to erase personal data where (i) individuals object to the processing of their personal data based on reasons relating to their particular situation under Article 21(1) of the GDPR, and (ii) data controllers cannot demonstrate that there are compelling legitimate reasons for the data processing, which override those reasons. The Guidelines should further explain that exceptions to

the right to erasure under Article 17 of the GDPR can be invoked as compelling legitimate grounds. CIPL recommends that on this basis, the Guidelines extend this position to the right to object generally (and not just in delisting cases) and that the following cases be confirmed – among other possible cases - as "compelling legitimate interests":

- Processing for the exercise of the right of freedom of expression and information;
- Processing for compliance with a legal obligation which requires processing by applicable law to which the controller is subject, or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- Processing for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) and Article 9(3);
- Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1);
- Processing for the establishment, exercise or defence of legal claims; and
- Processing for the prevention of fraud and for the protection of network and information security (in the meaning of Recitals 47 and 49 of GDPR).

This approach should also be taken into account in the updated version of the WP29 Opinion WP217 on the notion of legitimate interests of the data controller.

Summary of CIPL recommendations:

- Further clarify the rationale and limits of the right to object; and
- Expand the interpretation of the notion of "compelling legitimate interest" in Article 17(3) to Article 21(1).

CIPL is grateful for the opportunity to provide recommendations in the context of the EDPB's work on Guidelines on Data Subject Rights. If you would like to discuss any of these recommendations or require additional information, please contact Bojana Bellamy, bbellamy@huntonAK.com, Markus Heyder, mheyder@huntonAK.com, or Nathalie Laneret, nlaneret@huntonAK.com.