ANTI-CORRUPTION HELPDESK

PROVIDING ON-DEMAND RESEARCH TO HELP FIGHT CORRUPTION

THE IMPACT OF THE NEW GENERAL DATA PROTECTION REGULATION (GDPR) ON WHISTLEBLOWING

QUERY

We are looking for an analysis of the potential impact of the new General Data Protection Regulation on:

1. the right to confidentiality or anonymity of whistleblowers
2. the responsibility of employers, regulators or service providers (including Transparency International's Advocacy and Legal Advice Centres) to manage data shared by whistleblowers
3. the right of accused/respondents to be notified of any data and obtain data held on them that is shared by whistleblowers about them

CONTENT

1. Background
2. Decoding the GDPR
3. Impact of the GDPR on whistleblowing
4. References

Author(s)
Kaunain Rahman, tihelpdesk@transparency.org

Reviewer(s)
Marie Terracol, Matt Jenkins

Date: 30 April 2018

SUMMARY

The EU General Data Protection Regulation (GDPR) will come into force on 25 May 2018. It offers the most ambitious and far-reaching changes to data protection laws in Europe in the last 20 years, and has a truly global impact as any organisation in the world which sells to European companies, or receives data from EU citizens will be affected (Evans et al. 2016; Gross 2016).

With the objective of protecting the personal data of EU citizens, the resolution clearly outlines the meaning of personal data and consent, as well as highlighting the rights of individuals and the obligations on part of organisations that process personal data (Evans et al. 2016; White & Case 2016; EU GDPR Portal 2018; ICO 2018).

Whistleblowing (reporting of wrongdoing) is widely recognised for playing a crucial role in exposing corruption (Transparency International 2013). While the GDPR puts the whistleblower in a much stronger position and affords them more authority over their own data, there remain challenges such as the protection of the whistleblower's identity if the accused in the report demands access to their personal information recorded in the whistleblower's report. The GDPR will mean that whistleblowing processes need to change to ensure that the reporter is more informed and the potential for significant data breaches is reduced. This change is viewed by some as a positive development for both organisations handling personal data and for whistleblowers (Expolink 2017).

1. BACKROUND

Whistleblowing may be defined as the disclosure or reporting of wrongdoing, including but not limited to: corruption; criminal offences; breaches of legal obligation; miscarriages of justice; specific dangers to public health, safety or the environment; abuse of authority; unauthorised use of public funds or property; gross waste or mismanagement; conflict of interest; and acts to cover up of any of these (Transparency International 2013).

While whistleblowers play a crucial role in exposing corruption, fraud, mismanagement and other wrongdoing that threaten public health and safety, financial integrity, human rights, the environment and the rule of law, they often take on high personal risk when they do so (Goel and Nelson 2013; Transparency International 2013). To curtail these potential losses and encourage individuals to come forward in the detection of wrongdoing, countries have introduced various incentives, ranging from tokens of recognition to financial rewards (OECD 2016)

Whistleblower protection is the ultimate line of defence for safeguarding the public interest. Protecting whistleblowers promotes a culture of accountability and integrity in both public and private institutions, and encourages the reporting of misconduct, fraud and corruption (OECD 2016a).

Whistleblower protection should ensure that whistleblowers are protected against all forms of unfair treatment at the workplace (such as retaliation, disadvantage or detriment) but also outside of the workplace (such as legal actions) (Transparency International 2018).

Whistleblower protection legislation remains the exception rather than the rule in the EU, as most member states do not have dedicated legislation in place, and even in the few countries where such laws do exist, they usually leave significant loopholes and fall short of good practice (Centre for Media Pluralism and Media Freedom 2014; Transparency International EU 2017).

Various organisations, such as the Council of Europe, Organisation for Economic Co-operation and Development (OECD), Transparency International and the European Parliament, have pointed out that effective protection of whistleblowers is a critical tool to address corruption and other wrongdoings (Transparency International EU 2017). On 23 April 2018, the EU Commission issued a proposal for an EU directive to establish common minimum standards for the protection of persons reporting breaches in specific union policy areas. This is currently being discussed by the European Parliament and the Council.

The proposal for the directive states that a lack of whistleblower protection in a member state may not only have a negative impact on the functioning of EU policies in that state, but could also have spill-over effects in other member states. Moreover, as whistleblower protection at the EU level is fragmented and exists only in specific sectors to varying degrees, whistleblowers are left vulnerable to retaliation. Thus, the proposal for this directive aims to address these issues by a balanced set of common minimum standards providing robust protection (European Commission 2018b).

In particular, the proposal states that whistleblowers qualify for protection where

- they had reasonable grounds to believe that the information reported was true at the time of reporting
- internal channels do not work or could not reasonably be expected to work
- no appropriate action is taken or, in particular circumstances, such as imminent or manifest danger to the public interest

The proposal also outlines that member states ought to provide for proportionate sanctions to dissuade malicious reports and that those concerned by the reports fully enjoy the presumption of innocence, the right to an effective remedy, the right to a fair trial and the rights of defence.

In the majority of cases, the implementation of whistleblowing systems relies on the processing of personal data through the collection, registration, storage, disclosure, transmission and destruction of data related to an identified or identifiable person (OECD 2017). Thus, before getting into the impact that GDPR would have on whistleblowing it is imperative to understand what the GDPR encompasses.

2. DECODING THE GDPR

The EU General Data Protection Regulation (GDPR), over four years in the making, was approved on 14 April 2016 and published in the EU Official Journal on 4 May 2016 (Evans et al. 2016; EU GDPR Portal 2018). In essence, as denoted in Article 1 of the resolution, it relates to "the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data" (EU GDPR Portal 2018; Intersoft Consulting 2018). It applies directly to all EU member states as of 25 May 2018. It will repeal and replace the 1995 Data Protection Directive (95/46EC) and its member state implementing legislation. Along with the Directive on the Processing of Personal Data for the Purpose of Crime Prevention,[1] the GDPR offers the most ambitious and far-reaching changes to data protection laws around the world in the last 20 years (Evans et al. 2016).

Jurisdiction

The resolution applies to organisations located within the EU as well as those located outside of the EU if they offer goods or services to, or monitor the behaviour of EU data subjects (EU GDPR Portal 2018). It also applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location (EU GDPR Portal 2018).

The GDPR does not apply to certain activities, including data processing covered by the Law Enforcement Directive[2], processing for national security purposes and processing carried out by individuals purely for personal/household activities (ICO 2018).

The GDPR allows for data transfers to countries whose legal regime is deemed by the European Commission to provide for an "adequate" level of personal data protection (Iapp 2018). In the absence of an adequacy decision, however, transfers are also allowed outside non-EU states under certain circumstances, such as by use of standard contractual clauses or binding corporate rules (BCRs)[3] (Iapp 2018).

Defining critical terms

The GDPR (Regulation (EU) 2016/679) contains a number of new provisions, as well as modifying or even removing certain provisions that existed under the 1995 Data Protection Directive (DPD) (Chaturvedi 2017).

The GDPR redefines personal data and consent, providing stricter and broader definitions of these terms than the DPD. The GDPR also adds new individual rights. For instance, EU citizens will have to explicitly opt in to the storage, use and management of their personal data, and will have the right to access, amend, or request the deletion of their personal data. The EU GDPR also exclusively requires mandatory data breach notification to the individuals, and to a supervisory authority within 72 hours (Gross 2016; Chaturvedi 2017).

DPD provisions which have been omitted from the GDPR include the general obligation to notify processing supervisory authorities since it was observed that this requirement imposed unnecessary financial and administrative burdens on organisations. Instead, the GDPR is set to rely on procedures and mechanisms like privacy impact assessment to ensure compliance (Chaturvedi 2017). A new European Data Protection Board replaces the DPD's working party.

The following section defines key terms.

Personal data: refers to any information relating to an identified or identifiable natural person ("data subject")[4] who can be directly or indirectly identified by

[1] Passed on the same day as the GDPR.
[2] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (EUR-Lex 2018).
[3] With regard to BCRs and standard contract clauses, important distinctions between the GDPR and the directive bear noting. In particular, the GDPR explicitly acknowledges as valid the current requirements for BCRs for controllers and processors, which will be helpful for data transfers involving those member states that do not as yet recognise BCRs. Standard contractual clauses, which prior to the GDPR required prior notice to and approval by data protection authorities, may now be used without such prior approval. Further, a newly introduced scheme in the GDPR allows for transfers based upon certifications, provided that binding and enforceable commitments are made by the controller or processor to apply the appropriate safeguards (Iapp 2018).
[4] Data subject means an individual who is the subject of personal data (ICO 2018).

reference to location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person (EDPS 2018b; ICO 2018). It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address (EU GDPR Portal 2018). The resolution covers a wide range of personal identifiers, which encompass changes in technology and the way organisations collect information about people (ICO 2018).

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria, this could include chronologically ordered sets of manual records containing personal data (EU GDPR Portal 2018; ICO 2018).

Personal data that has been "pseudonymised" can fall within the scope of the GDPR depending on how challenging it is to connect the pseudonym to a particular individual (ICO 2018).

Sensitive personal data: these are "special categories of personal data" which are subject to additional protections and require organisations to have stronger grounds to process them (White & Case 2016). These include genetic data, and biometric data, or those that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life (White & Case 2016; ICO 2018). Although personal data relating to criminal convictions and offences are not included,[5] and may only be processed by national authorities, similar extra safeguards apply to their processing (White & Case 2016; ICO 2018).

Pseudonymous data: these comprise data that may be altered in such a way that no individuals can be identified from those data (whether directly or indirectly) without a "key" that allows the data subject to be re-identified (White & Case 2016).

If the "key" that enables re‑identification of individuals is kept separate and secure, the risks associated with pseudonymous data are likely to be lower, and so the levels of protection required for those data are likely to be lower (White & Case 2016).[6] Thus, pseudonymisation of data provides advantages: it can allow organisations to satisfy their obligations of "privacy by design" and "privacy by default" and it may be used to support processing that would otherwise be considered "incompatible" with the purposes for which the data were originally collected (White & Case 2016). The GDPR explicitly encourages organisations to consider pseudonymisation as a security measure (White & Case 2016).

Controllers and processors: a controller means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. Where the purposes and means of processing are determined by EU or member state laws, the controller (or the criteria for nominating the controller) may be designated by those laws (White & Case 2016; EU GDPR Portal 2018; ICO 2018).

A processor is responsible for processing personal data on behalf of a controller (EU GDPR Portal 2018; ICO 2018). In the case of a processor, the GDPR places specific legal obligations on them. For example, they are required to maintain records of personal data and processing activities and will have legal liability if they are found responsible for a breach (ICO 2018). The controller, however, does not get relieved of their obligations by involving a processor, the GDPR is clear in placing further obligations on the former to ensure that contracts with the latter comply with the resolution (ICO 2018).

The European Commission (2018d) chooses to explain these terms with the following example. A brewery has many employees. It signs a contract with a payroll company to pay the wages. The brewery tells the payroll company when the wages should be paid,

[5] The rules under the GDPR in relation to data concerning criminal convictions and offences mirror those which applied under the DPD, they are not categorised as "sensitive" for the purposes of GDPR (although the UK Data Protection Act treats personal data relating to criminal proceedings and convictions as sensitive data). The GDPR provides that such data may be processed only under the control of official authority or where the processing is authorised by union law or member state law that provides appropriate safeguards. This provision is likely to lead to continued national divergence in this area (Bird & Bird 2017).

[6] The current EU directive on data protection does not recognise any distinction between regular personal data and pseudonymised data. The GDPR on the other hand, specifically promotes the value and importance of pseudonymisation throughout its articles, encouraging organisations to adopt such security measures as soon as possible. The areas in which organisations could benefit from pseudonymisation include reduction of data breach notification requirements, an easing of data disclosure obligations, and further use of data beyond its original purpose (Kefron 2017).

when an employee leaves or has a pay rise, and provides all other details for the salary slip and payment. The payroll company provides the IT system and stores the employees' data. The brewery is the data controller and the payroll company is the data processor.

Consent: means any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed (White & Case 2016).

The GDPR makes it significantly harder for organisations to obtain valid consent from data subjects, and for organisations that rely on consent for their business activities, the processes by which they obtain consent will need to be reviewed and revised to meet the requirements of the GDPR (White & Case 2016).

As stated, the GDPR sets a high standard for consent. Consent means offering individuals real choice and control, and requires a positive opt-in (ICO 2018). Explicit consent requires a very clear and specific statement of consent and pre-ticked boxes or any other method of default consent do not apply (ICO 2018). Specificity for what consent is being awarded is also a requirement; it ought to be "granular" so that separate consent is obtained for separate aspects (ICO 2018). Vague or blanket consent is not enough (ICO 2018).

Another requirement is to make it easy for people to withdraw consent (ICO 2018). Moreover, for companies it is imperative that they keep evidence of consent – who, when, how, and what they told people (ICO 2018).

For children below the age of 16, parental consent will be required to process their personal data for online services; member states may legislate for a lower age of consent but not below the threshold age of 13 (EU GDPR Portal 2018).

Data protection authorities (DPA): DPAs (supervisory authorities) are independent public authorities that supervise, through investigative and corrective powers, the application of the data protection law (Evans et al. 2016; European Commission 2018c). They are mandated to respond to complaints and enforce the GDPR and local data protection laws for data subjects affected in the member state that the authorities overlook (Evans et al 2016). In the case of cross-border processing, a lead supervisory authority system (determined by the location of the "main establishment"[7] of the organisation) applies, through which that authority enforces the GDPR in consultation with the other "concerned" DPAs (Evans et al. 2016).

The GDPR lays down detailed provisions on supervisory authorities, defining their functions, independence, appointment of members, establishment rules, competence of lead supervisory authority, tasks, powers and activity reports, such elaborate provisions are absent in the DPD (Chaturvedi 2017).

DPAs provide expert advice on data protection issues and handle complaints lodged against violations of the GDPR and the relevant national laws (European Commission 2018c).

Data Protection Officer (DPO): is a person who is formally tasked with ensuring that an organisation is aware of, and complies with, its data protection responsibility (White & Case 2016). DPOs ought to be appointed in the case of (a) public authorities, (b) organisations that engage in large scale systematic monitoring, or (c) organisations that engage in large scale processing of sensitive personal data (EU GDPR Portal 2018).

The DPO should report to the highest management level of the controller or processor (as appropriate) and must be supported in carrying out their functions, including with the necessary resources and the DPO's contact details must be notified to the supervisory authority (DPA) so that they will be the first official contact point on any issues (Evans et al 2016).

European Data Protection Supervisor (EDPS): is the European Union's independent data protection authority.

[7] The main establishment of a controller in the union should be the place of its central administration in the union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the union, in which case that other establishment should be considered to be the main establishment (Intersoft Consulting 2018).

Privacy by design and by default: under the GDPR, controllers and processors have a general obligation to implement technical and organisational measures to show that they have considered and integrated data protection into their processing activities (Evans et al. 2016; ICO 2018).

At the conceptual level, data protection by design and default mean that privacy should be a feature of the development of a product, rather than something that is tacked on later. The GDPR for the first time introduces the concept of "data protection by design" into formal legislation. Thus, the GDPR requires controllers to implement appropriate safeguards "both at the time of the determination of the means for processing and at the time of the processing itself". Measures to enable these concepts may include: minimisation of processing, pseudonymisation, transparency while processing, and allowing data subjects to monitor data processing (Maldoff 2016; Chaturvedi 2017).

Data processing principles

Although the changes introduced by the GDPR to the Data Protection Principles are not revolutionary, certain concepts are more fully developed and they do consolidate the importance of those principles in respect of data processing activities (Taylor Wessing 2016; White & Case 2016). In particular, the principles of transparency and minimisation of data, as well as the requirement of data integrity and confidentiality, are now clearly established as Data Protection Principles (White & Case 2016). The following principles apply to the processing of personal data:

Lawfulness, fairness and transparency: data ought to be processed lawfully, fairly and in a transparent manner in relation to the data subject (Taylor Wessing 2016). A method of achieving transparency is keeping the individual informed before data is collected and where any subsequent changes are being made (Taylor Wessing 2016).

Purpose limitation: processing personal data is only permissible if and to the extent that it is compliant with the original purpose for which data was collected (Taylor Wessing 2016). Processing "for another purpose" later requires further legal permission or consent (Taylor Wessing 2016). The only exception being that the "other purpose" is "compatible" with the original purpose (Taylor Wessing 2016).

Data minimisation: data controllers are to ensure that only personal data, which is necessary for each specific purpose, is processed (in terms of the amount of personal data collected, the extent of the processing, the period of storage and accessibility) (Taylor Wessing 2016). Under the GDPR, data must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" (Taylor Wessing 2016). This ties back to the purpose limitation (Taylor Wessing 2016). Controllers need to make sure that they collect enough data to achieve their purpose but not more than is needed (Taylor Wessing 2016).

Accuracy: the GDPR states that personal data shall be accurate and, where necessary, kept up to date (Taylor Wessing 2016).

Storage limitation: personal data is to 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 (Taylor Wessing 2016). A regular review process may be put in place with methodical cleansing of databases to meet this principle (Taylor Wessing 2016).

Integrity and confidentiality: personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (Taylor Wessing 2016).

Accountability: the controller shall be responsible for, and should be able to demonstrate, compliance with the GDPR (Taylor Wessing 2016).

Rights of individuals

The GDPR provides the following rights for individuals:

The right to be informed: a key transparency requirement under the GDPR is that individuals have the right to be informed about the collection and use of their personal data (White & Case 2016; ICO 2018). The information must include the purposes for processing their personal data, the retention periods

for that personal data, and who it will be shared with, this is termed "privacy information", which must be provided to individuals at the time their personal data is collected from them (White & Case 2016; ICO 2018).

In case processors obtain personal data from other sources, they must provide the data subject with privacy information[8] within a reasonable period of obtaining the data and no later than one month (ICO 2018).

The information that is provided to people ought to be concise, transparent, intelligible, easily accessible, and it must use clear and plain language (ICO 2018). It is often most effective to provide privacy information to people using a combination of different techniques including layering, dashboards and just-in-time notices (ICO 2018).

The right of access: under the GDPR, individuals will have the right to obtain a confirmation that their data is being processed, access to their personal data and other supplementary information – which largely corresponds to the information that should be provided in a privacy notice (when they are being informed) (ICO 2018). Allowing individuals to access their personal data means that they are aware of and can verify the lawfulness of the processing as well as the correctness of information (ICO 2018).

A copy of the information must be provided free of charge. However, in the case of manifestly unfounded or excessive, particularly repetitive requests, processors can charge a "reasonable fee" (this is limited to requests for further copies of the same information and does not mean that all subsequent access requests would be charged) (ICO 2018). The fee charged should also only cover the administrative cost of providing the information (ICO 2018).[9]

The current Data Protection Directive (since 1995) and the GDPR both note that the exercise of the right of access by data subjects should not adversely affect an organisation's intellectual property (that is, giving the right of access should not require the disclosure of trade secrets), while also noting such occurrences of this happening would be rare (White & Case 2016).

The right to rectification: controllers must ensure that inaccurate or incomplete data are erased or rectified. Data subjects have the right to rectification of inaccurate personal data, either verbally or in writing and they must receive a response within one month from placing such a request (White & Case 2016; ICO 2018). This right is closely linked to the principle of accuracy (ICO 2018).

The right to erasure (the right to be forgotten): this right is not absolute and only applies in certain circumstances, as follows (White & Case 2016; ICO 2018):

- the data are no longer needed for their original purpose (and no new lawful purpose exists)
- the data subject withdraws consent, and the controller has no overriding grounds for continuing the processing
- the data has been processed unlawfully
- erasure is necessary for compliance with EU law or the national law of the relevant member state

Individuals can make a request for erasure verbally or in writing, controllers have one month to respond to a request (ICO 2018).

The right to restrict processing: data subjects have the right to restrict the processing of personal data (meaning that the data may only be held by the controller, and may only be used for limited purposes) in the following circumstances (White & Case 2016; ICO 2018):

- the accuracy of the data is contested (and only for as long as it takes to verify that accuracy)
- the processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure)
- the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights

[8] Privacy information includes the organisation's purposes for processing an individual's personal data, their retention period for that personal data and with whom it will be shared (ICO 2018).

[9] The GDPR includes a best practice recommendation that, where possible, organisations should be able to provide remote access to a secure self-service system, which would provide individuals with direct access to their information (Recital 63). This will not be appropriate for all organisations, but there are some sectors where this may work well (ICO 2018).

- if verification of overriding grounds is pending, in the context of an erasure request

The right to data portability: this right allows individuals to obtain, reuse, move, copy or transfer their personal data for their own purposes across different services in a safe and secure way, without hindrance to usability (White & Case 2016). It enables consumers to take advantage of applications and services which can use this data to find them a better deal or help them understand their spending habits (White & Case 2016).

Inferred data and derived data (for example, a credit score or the outcome of a health assessment) do not fall within the right to data portability, because such data are not "provided by the data subject" (ICO 2018). In addition, the controller is not obliged to retain personal data for longer than is otherwise necessary, simply to service a potential data portability request (ICO 2018).

The right to object: individuals have the right to object to the following (ICO 2018):

- processing based on legitimate interests of the controller or the performance of a task in the public interest/exercise of official authority (including profiling)
- direct marketing
- processing for purposes of scientific/historical research and statistics

The earlier 1995 directive permitted an organisation to continue processing the relevant data unless the data subject can show that the objection is justified (White & Case 2016). The GDPR reverses the burden and requires the organisation to demonstrate that it either has compelling grounds for continuing the processing or that the processing is necessary in connection with its legal rights (White & Case 2016). In case it fails to showcase that the relevant processing activity falls within one of these two grounds, it must cease that processing activity (White & Case 2016).

Rights in relation to automated decision making and profiling: data subjects have the right not to be subject to a decision based solely on automated processing which significantly affects them (including profiling). Such processing is permitted where (Taylor & Case 2016):

- it is necessary for entering into or performing a contract with the data subject provided that appropriate safeguards are in place
- it is authorised by law
- the data subject has explicitly consented and appropriate safeguards are in place

Penalties

Penalties for non-compliance with the GDPR include a fine of up to 4 per cent of annual global turnover or €20 million. This is the maximum fine that can be imposed for the most serious infringements, for example, for not having sufficient customer consent to process data or violating the core of privacy by design concepts. A tiered approach to fines has also been stipulated. For example, a company can be fined 2 per cent of their turnover for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting an impact assessment. It is important to note that these rules apply to both controllers and processors, meaning "clouds" will not be exempt from GDPR enforcement.

3. IMPACT OF THE GDPR ON WHISTLEBLOWING

Whistleblowing in the EU against the backdrop of the GDPR

As mentioned earlier, more often than not, the implementation of whistleblowing systems on the processing of personal data through the collection, registration, storage, disclosure, transmission and destruction of data is related to an identified or identifiable person (OECD 2017). Thus, data protection requirements need to be balanced against secure and effective whistleblowing systems (OECD 2017).

The erstwhile Data Protection Directive as well as the soon to be enforced GDPR require bodies which set up whistleblowing systems to comply with the requirements of notification to, or prior checking by, the national DPA (OECD 2017). In fact, the GDPR has tighter data protection provisions and requires stronger enforcement of those provisions both by companies and by regulators (OECD 2017).

The GDPR is therefore set to have a wide-reaching impact on internal reporting mechanisms within companies, and the DPA will have an increased role in oversight and monitoring of their effectiveness (OECD 2017). The DPA will also be responsible for receiving complaints of employees who consider their data protection rights to have been violated as a consequence of whistleblower disclosures (OECD 2017).

A study conducted by the OECD/G20 on G20 Whistleblower Protection Frameworks had found that the earlier data protection laws (pre-GDPR) in some countries might impose legal restrictions on internal private sector whistleblowing procedures (OECD 2016b). In some countries, like Denmark, private organisations are adopting internal reporting mechanisms, and then getting them approved by their national DPA (OECD 2016b). In other cases, like France, courts have invalidated internal whistleblowing procedures for being too broad in scope and potentially violating data protection laws (OECD 2016b). This illustrates the current fragmentation of whistleblower protection laws across the EU.

The proposal for a EU directive on establishing common minimum standards for the protection of persons reporting on breaches in specific EU policy areas (published on 23 April 2018) seeks to pursue a balanced approach to ensure the full respect of further rights that may be affected, such as the right to a private life and to the protection of personal data of whistleblowers but also of the people concerned by the reports, as well as the presumption of innocence and the rights of defence (European Commission 2018b).

The proposal states that the processing of data relating to whistleblower reports should be done in accordance with the GDPR (European Commission 2018b). It further specifies that personal data, which are not relevant for the handling of a specific case, should be immediately deleted.

Nevertheless, the proposal also recognises protection of privacy and personal data as significant areas where whistleblowers are in a position to disclose breaches of EU law (European Commission 2018b).

Citing the example of the Cambridge Analytica scandal, where there were significant breaches of the EU data protection rules (including acquisition of data without consent of tens of millions of individuals concerned and use of the personal data for a different purpose than the one for which it was collected), an impact assessment of the proposal states that it was indeed a whistleblower that brought this wrongdoing to light (European Commission 2018a).

Thus, the impact assessment goes on to highlight that the proposed whistleblowing directive would help improve data protection as whistleblowers "remain a particularly valuable source of information to unmask certain types of infringements which are particularly harmful to the public interest" (European Commission 2018a).

The protection of whistleblowers' identity (right to confidentiality or anonymity of whistleblowers)

When it comes to ensuring the protection of a whistleblower's identity, Transparency International (2018) notes that there are two different approaches: preserving confidentiality and allowing anonymous reporting. Transparency International notes that confidentiality is a minimum requirement of any legislation that aims to protect whistleblowers, and that guaranteeing the former will also incidentally help reduce the need for anonymous reporting.

In 2016, the European Data Protection Supervisor (EDPS) published Guidelines on Processing Personal Information within a Whistleblowing Procedure. This document stipulates that EU institutions should manage whistleblowing reports to ensure the protection of the personal information of the whistleblowers, the alleged wrongdoers, the witnesses and the other persons appearing in the report.

It ought to be noted that these guidelines officially only apply to EU institutions, and while they are helpful to understand the impact of the GDPR on whistleblowing systems, they are in no case directly applicable to national public institutions or private companies.
The EDPS guidelines state that the identity of the whistleblower who reports serious wrongdoings or irregularities in good faith should be treated with the utmost confidentiality (EDPS 2016). Their identity should never be revealed except in certain exceptional

circumstances: if the whistleblower authorises such a disclosure, if this is required by any subsequent criminal law proceedings, or if the whistleblower maliciously[10] makes a false statement. In the latter case, these personal data can only be disclosed to judicial authorities (EDPS 2016).

When it comes to the storage period for whistleblowing reports, the period may vary significantly depending on the complexity of an investigation (Expolink 2017). Although a "set retention period" is not always applicable, whistleblowers should be advised that their details would only be retained until the case is closed and the issue resolved (Expolink 2017).

Data subjects have the right to access their personal data, especially where the personal data is not collected from the data subject, they could demand any information held as to its source (Expolink 2017). This may risk exposing a whistleblower's identity, which is a key concern. A scenario where the person who is the object of a whistleblowing disclosure could discover the identity of the whistleblower, if they are given access to their own data (the whistleblower report, for example), is an area of concern for the GDPR's impact on whistleblowing.

While the Article 29 Working Party[11] recommends "under no circumstances can the person accused in a whistleblower's report obtain information about the identity of the whistleblower", the term recommendation in itself is problematic as a recommendation is not enforceable (Expolink 2017). The risks for not following the recommendation would include violating the minimum confidentiality requirement, which stands as a first line of protection in the whistleblowing system (Transparency International 2018). While there is provision under the resolution for member states to restrict the GDPR subject rights for the "prevention, investigation, detection or prosecution of criminal offences" or civil law claims, currently, no provisions have yet been enacted or even drafted (Expolink 2017).

Furthermore, any personal information related to whistleblowing retained for statistical purposes should be made anonymous (EDPS 2016). The EDPS guidelines specifically warn EU institutions to be particularly cautious with any information that may result in indirect identification; for example, retaining both the type of whistleblowing cases together with the nationality of the whistleblower could lead to indirect identification and should, therefore, be avoided (EDPS 2016).

Responsibility of employers, regulators, or service providers, including Transparency International's Advocacy and Legal Advice Centres, to manage data shared by whistleblowers

Reviews are currently underway regarding the impact of the GDPR on national legal guidelines for internal whistleblowing systems in EU countries where such guidelines exist. The EDPS guidelines establish that the purpose of the whistleblowing procedure must be clearly specified in the internal rules/policy of EU institutions so as to allow data subjects to be better informed (EDPS 2016; WhistleB 2016). The internal rules or a policy should furthermore describe that collection of sensitive information not relevant to the case must be avoided (EDPS 2016).

All controllers and processors ought to follow the aforementioned data processing principles under the GDPR (lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability), strictly following data minimisation.

The challenge however remains that, when capturing a whistleblowing report, greater detail can greatly aid the investigation process, but it can be difficult to determine how much information is 'too much' (Expolink 2017).

[10] A statement is maliciously made if whistleblowers report activities that they know are not true (EDPS 2016). If an EU institution becomes aware of that whistleblowers knew that the allegation the made was unsubstantiated, the responsibility lies with the institution to prove the maliciousness of the allegations (EDPS 2016).

[11] The "Article 29 Working Party" is another name for the Data Protection Working Party established by Article 29 of Directive 95/46/EC. It provides the European Commission with independent advice on data protection matters and helps in the development of harmonised policies for data protection in EU member states. The Working Party is composed of: representatives of the national supervisory authorities in the member states; a representative of the European Data Protection Supervisor (EDPS); and a representative of the European Commission (the latter also provides the secretariat for the working party) (EDPS 2018a).

Some suggest that the solution to this challenge may be that, as reporters are keen to protect themselves, and non-compliant processors and controllers facing heavy fines under GDPR, both parties will be motivated to avoid unnecessary personal data being shared (and subsequently stored and processed) (Expolink 2017).

Organisations need to ensure that their whistleblowing system that deals with personal data meets the stricter technical and organisational requirements in the new regulations (WhistleB 2016).

These include:

- Privacy by design: data protection and data privacy should permeate the design and processes of the whistleblowing system. It is important to ensure secure data processing, storage and destruction (including back-ups) (WhistleB 2016).
- Privacy by default: the whistleblowing system by default should enable the highest level of data privacy and protection in the handling of personal data (WhistleB 2016).
- Organisations need to ensure that they have a process and technical system in place for "pseudonymisation" to ensure personal data security when an external processor is involved (WhistleB 2016).
- Obligation to notify data breaches: there is a new obligation for controllers to notify the relevant authorities of data breaches within 72 hours, and to communicate such breaches to the data subjects (WhistleB 2016). Processors are obliged to notify the controller (WhistleB 2016).
- Organisations need to have a personal data processor agreement in place if they outsource the processing of whistleblowing cases (WhistleB 2016).
- They should also consider placing a requirement on the processor that they have an appointed DPO (if they meet the criteria: please refer to the section above on definitions) (WhistleB 2016).
- The GDPR will be applicable to companies established outside the EU (both controllers and processors) if they monitor the behaviour of EU data subjects within the EU. There is an obligation for them to appoint a representative in the EU (WhistleB 2016).
- Organisations should ensure documentation exists regarding correct data processing, both for controllers and processors (WhistleB 2016).
- Detailed documentation of data processing (accountability) should be maintained in a secure way, both by controllers and processors (WhistleB 2016).
- Making the whistleblowing privacy notice/policy and other information easily available (which can be easily understood) to all parties invited to report (WhistleB 2016).
- Provide contact details of the data controller responsible for the whistleblowing system, and when appropriate, details of the DPO (WhistleB 2016). This information should also be documented (WhistleB 2016).
- Inform employees about potential other recipients or categories of recipients that may have access to personal data in the whistleblower report. For example, if the data or investigations have been outsourced. Employees should also be informed of potential recipients of personal data outside the EU/EEA area.

Right of accused/respondents to be notified of any data and obtain data held on them that is shared by whistleblowers about them

The person against whom an allegation has been made should be protected in the same manner as the whistleblower, since there is a risk of stigmatisation and victimisation within their organisation (EDPS 2016). They will be exposed to such risks even before they are aware that they have been incriminated and the alleged facts have been analysed to determine whether or not they can be sustained (EDPS 2016).

The EDPS notes that, in certain cases, informing the person against whom an allegation has been made at an early stage may be detrimental to the case (EDPS 2016). In these cases, provision of specific information might need to be deferred. However, deferral of information should be decided on a case-by-case basis (EDPS 2016). The reasons for any restrictions include, for instance, that there is a high risk that giving access would hamper the procedure or undermine the rights and freedom of the others (EDPS 2016). The reasons should be documented before the decision to apply any restriction or deferral is taken (EDPS 2016).

Preserving the rights of a data subject where he/she is the accused is challenging. The biggest potential stumbling block is where consent is withdrawn, while providers should be able to remove personal data from reports; investigation of the report may be more difficult without this information (Expolink 2017). Finally, with the accused's right to object: it is not uncommon for a report to have a legal foundation or criminal aspect to the subject of the report, therefore, the right to object under GDPR may be countered on this basis (Expolink 2017).

Road ahead

As the data subject, GDPR puts the whistleblower in a much stronger position and affords them more authority over their own data (Expolink 2017). In doing so it may mean that whistleblowing processes need to change, but it will do so in a way that means the whistleblower is more informed and the potential for significant data breaches is reduced. This can be viewed as a positive development for both organisations that handle personal data as well as whistleblowers themselves (Expolink 2017).

The interaction of the proposed EU-wide whistleblowing directive (once it comes into force) with the GDPR and the impact it will have on personal data protection in practice remains to be seen. For now, as stated in the impact assessment of the proposal of the whistleblowing directive, whistleblowing remains a significant area in helping data protection, while data protection in turn, boosts the confidentiality principle that is critical to a sound whistleblowing mechanism (European Commission 2018a; Transparency International 2018).

4. REFERENCES

Bird & Bird. 2017. *Guide to the General Data Protection Regulation*. https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en

Centre for Media Pluralism and Media Freedom. 2014. *Whistleblowing Protection Laws – EU Member States Laws*. http://journalism.cmpf.eui.eu/maps/whistleblowing/

Chaturvedi, A. 2017. *Comparison of General Data Protection Regulation and Data Protection Directive*. *The Centre for Internet and Society.* https://cis-india.org/internet-governance/blog/comparison-of-general-data-protection-regulation-and-data-protection-directive

EUR-Lex. 2018. *EUR-Lex – 32016L0680*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG

EU GDPR Portal. 2018. *Key Changes with the General Data Protection Regulation* https://www.eugdpr.org/the-regulation.html

European Commission. 2018a. *Commission Staff Working Document – Impact Assessment Accompanying the Document – Proposal for a Directive of the European Parliament and of the Council on the Protection of Persons Reporting on Breaches of Union Law*.

European Commission. 2018b. *Proposal for a Directive of The European Parliament and of The Council on the protection of persons reporting on breaches of Union law*. https://ec.europa.eu/info/sites/info/files/placeholder_8.pdf

European Commission. 2018c. *What are Data Protection Authorities (DPAs)?* https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en

European Commission. 2018d. *What is a Data Controller or a Data Processor?* https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en

European Data Protection Supervisor (EDPS). 2016. *Guidelines on Processing Personal Information Within a Whistleblowing Procedure*. https://edps.europa.eu/sites/edp/files/publication/16-07-18_whistleblowing_guidelines_en.pdf

European Data Protection Supervisor (EDPS). 2018a. *Data Protection – Definition of Personal Data* https://edps.europa.eu/data-protection/data-protection/glossary/p_en

European Data Protection Supervisor (EDPS). 2018. *European Data Protection Supervisor – Article 29 Working Party*. https://edps.europa.eu/data-protection/data-protection/glossary/a_en

Evans, M., Nowak, J., Modrall, J., Martin, N., Nagelkerke, F., D'Haultfoeuille, M., Ritzer, C., Schreiber, L., Byrne Hill, M. and Koning, N. 2016. *GDPR Checklist. Norton Rose Fulbright LLP.* https://www.dataprotectionreport.com/wp-content/uploads/sites/489/2016/05/GDPR_Checklist_Norton_Rose_Fulbright_May_2016.pdf

Expolink. 2017. *How Will GDPR Affect the Whistleblowing Process?*

https://www.expolink.co.uk/blog/will-gdpr-affect-whistleblowing-process/

Goel, R. and Nelson, M. 2013. *Effectiveness of Whistleblower Laws in Combating Corruption. BOFIT Discussion Papers.* https://helda.helsinki.fi/bof/bitstream/handle/123456789/8010/171843.pdf?sequence=1

Gross, Z. 2016. *8 Ways EU GDPR Differs from the EU Data Protection Directive*. CloudLock. https://www.cloudlock.com/blog/eu-gdpr-vs-data-protection-directive/

Iapp. 2018. *Top 10 Operational Impacts of the GDPR: Part 4 – Cross-Border Data Transfers*. https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-4-cross-border-data-transfers/

ICO. 2018. *Guide to the General Data Protection Regulation (GDPR).* https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/

Intersoft Consulting. 2018. *General Data Protection Regulation (GDPR)*. https://gdpr-info.eu/art-1-gdpr/

Kafteranis, D. 2017. *Protection of Whistleblowers in the European Union: The Promising Parliament Resolution and the Challenge for the European Commission. Oxford Law Faculty.* https://www.law.ox.ac.uk/business-law-blog/blog/2017/12/protection-whistleblowers-european-union-promising-parliament

Kefron. 2017. *Data Masking & The GDPR: How Will Your Business Be Affected?* https://www.kefron.com/blog/data-masking-gdpr-how-will-businesses-be-affected/

Maldoff, G. 2016. *Top 10 Operational Impacts of the GDPR: Part 8 – Pseudonymization*. https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-8-pseudonymization/

OECD. 2016. *Committing to Effective Whistleblower Protection – Highlights*. http://www.oecd.org/corporate/committing-to-effective-whistleblower-protection-9789264252639-en.htm

OECD. 2016. *Committing to Effective Whistleblower Protection*. https://read.oecd-ilibrary.org/governance/committing-to-effective-whistleblower-protection_9789264252639-en#page3

OECD. 2017. *Greece-OECD Project: Technical Support on Anti-Corruption. Whistleblower Protection in the Private Sector: Developing the Legal Framework*. http://www.oecd.org/corruption/anti-bribery/OECD-Greece-Whistleblower-Protection-Forum-October-2017.pdf

Regulation. 2016. *Unlocking the EU General Data Protection Regulation | White & Case LLP International Law Firm, Global Law Practice*. https://www.whitecase.com/publications/article/chapter-5-key-definitions-unlocking-eu-general-data-protection-regulation

Taylor Wessing. 2016. *The Data Protection Principles under the General Data Protection Regulation*. https://www.taylorwessing.com/globaldatahub/article-the-data-protection-principles-under-the-gdpr.html

The Association of Chartered Certified Accountants (ACCA). 2018. *People Who Speak-Up Should Feel Safe to Do So, Says ACCA*. http://pr.euractiv.com/pr/people-who-speak-should-feel-safe-do-so-says-acca-166635

The World Law Group. 2016. *Global Guide to Whistleblowing Programs*. http://www.theworldlawgroup.com/Document.asp?DocID=116088

Transparency International EU. 2017. *EU Whistleblower Protection*. https://transparency.eu/wp-content/uploads/2017/11/EU-Whistleblower-Protection_Brief.pdf

Transparency International. 2013. *International Principles for Whistleblower Legislation*. https://www.transparency.org/whatwedo/publication/international_principles_for_whistleblower_legislation

Transparency International. 2018. *A Best Practice Guide for Whistleblowing Legislation.* https://www.transparency.org/whatwedo/publication/best_practice_guide_for_whistleblowing_legislation

WhistleB. 2016. *How to Handle Personal Data in a Whistleblowing System | Are You Compliant with the New EU General Data Protec on Regulation?* https://eben--net-fi-bin.directo.fi/@Bin/b16b2df9afc68a46764bee4eab890d3e/1523947205/application/pdf/183567/WhistleB_GDPR%26whistleblowing.pdf

"Anti-Corruption Helpdesk Answers provide practitioners around the world with rapid on-demand briefings on corruption. Drawing on publicly available information, the briefings present an overview of a particular issue and do not necessarily reflect Transparency International's official position."