EU Whistleblowing Legislation FAQs

Date : May 27, 2021

https://youtu.be/-srMzEoA1rU

We first published these FAQs in June 2020 and we have made some changes to reflect more recent developments

Introduction

In 2019 the EU introduced a new law to enable whistleblowers to report about EU law irregularities – this law also harmonises the minimum level of protection available to whistleblowers across the EU. These new rules are set out in "Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of [European] Union law" ("EU whistleblowing rules"). Because these new rules are in the form of a Directive this means that it is for EU countries to implement the obligations, procedures, protections etc. into national law. These FAQs set out the main aspects of these rules along with a particular focus on the data protection whistleblowing considerations with whistleblowing.

What is whistleblowing?

Whistleblowing is when an individual (typically an employee) discloses wrongdoing that has taken place within their organisation which the whistleblower reports to their organisation, governmental authorities or the media. In order to enable whistleblowing, whistleblowers are subject to a number of legal protections in some countries. The compliance and regulatory framework for whistleblowing may vary according to the context, for example as regards the employer-employee relationship or in a particular sector such as financial services. Whistleblowing also raises legal and compliance issues in other areas, notably data protection.

Why is the EU tackling whistleblowing?

Whistleblowing has been regulated comprehensively only in some EU countries and partially in others. Following scandals disclosed through whistleblowing between 2015 and 2018 such as the Dieselgate and Panama Papers matters, the EU introduced a raft of measures to address whistleblowing at an EU-wide level in order to enable the detection, investigation and sanction of abuses of EU law.

What laws and areas of EU law fall in scope?

The EU whistleblowing rules cover breaches in a wide number of areas of EU law ("relevant EU law"), which in the main are as follows:

- Public procurement;
- Financial services, products and markets, and prevention of money laundering and terrorist financing;
- Product safety and compliance;
- Transport safety;
- Protection of the environment;
- Radiation protection and nuclear safety;
- Food and feed safety, animal health and welfare;
- Public health;
- Consumer protection;
- Protection of privacy and personal data, and security of network and information systems; and
- EU internal market rules, including those concerning competition, State aid and corporate tax respectively.

The list of EU laws in the above areas is set out in detail in an annex to the EU whistleblowing rules.

What areas of EU and national law are not affected?

The EU whistleblowing rules do not affect the application of either EU law or national law relating to any of the following areas:

- The protection of classified information;
- The protection of legal and medical professional privilege;
- The secrecy of judicial deliberations; and
- Rules on criminal procedure.

Who can be a whistleblower?

Individuals who can be considered to be whistleblowers under the EU whistleblowing rules are as follows:

- Workers, as defined under EU law;
- The self-employed, as defined under EU law;
- Shareholders of an undertaking;
- Members of the management body of an undertaking, including non-executive members as well as volunteers and paid or unpaid trainees; and
- Anyone working under the supervision and direction of contractors, subcontractors and suppliers of an undertaking.

Further, under the EU whistleblowing rules, individuals may be considered to be whistleblowers:

- Where they report or publicly disclose information on breaches acquired in a work-based relationship which has since ended; and
- Whose work-based relationship is yet to begin in cases where information on breaches has been acquired during the recruitment process or other pre-contractual negotiations.

What is meant by reporting and disclosure?

Under the EU whistleblowing rules key reporting and disclosure terms are understood as follows:

- ‘Report’ or ‘to report’ means either the oral or written communication of ‘information on breaches’ – a whistleblower is a “reporting person” and whistleblowing is “reporting”;
- ‘Breaches’ means acts or omissions that are either unlawful and relate to the relevant EU law or defeat the object or purpose of relevant EU law;
- ‘Information on breaches’ means information, including reasonable suspicions, about actual or potential breaches of the relevant EU law, which occurred or are very likely to occur in the organisation in which the whistleblower works or has worked or in another organisation with which the whistleblower is or was in contact through their work, and about attempts to conceal those breaches;
- ‘Internal reporting’ means the oral or written communication of information on breaches within a private or public sector organisation and ‘external reporting’ means the oral or written communication of information on breaches to governmental authorities; and,
- ‘Public disclosure’ or ‘to publicly disclose’ means making ‘information on breaches’ available in the public domain.

Under what conditions is a whistleblower protected?

Individuals qualify for protection under the EU whistleblowing rules so long as:

1. They had reasonable grounds to believe that the ‘information on breaches’ reported was true at the time of reporting and that such information fell within the scope of the EU whistleblowing rules; and
2. They reported either internally, externally or made a public disclosure in accordance with the conditions of the EU whistleblowing rules specifically concerning these three areas (see below).

What about anonymous whistleblowing?

Without prejudice to existing obligations to provide for anonymous reporting by virtue of EU law, the EU whistleblowing rules do not affect the power of EU countries to decide whether organisations in the private or public sector and authorities are required to accept and follow up on anonymous reports of breaches – so it will be up to each country to decide on whether to allow for anonymous reporting or not and if so under what conditions.

It is important to remember that this has been an area of contention in the EU previously. There's a history of some of this litigation from 2005 here https://bit.ly/3htKadW. In-country legislation in some parts of the EU can be complicated and may dictate (amongst other things):

1. They types of issues a whistleblower may report anonymously;
2. Who may receive a report (for example in some countries some details may not be transmitted outside the country);
3. How a helpline is advertised;
4. The notice those being reported should be given;
5. The involvement of works councils;
6. How long reports can be retained for; and
7. Whether a helpline can be used for issues or whether a helpline can only be used when other channels have failed

Conflicts can also be magnified by the payment of bounties to whistleblowers in some countries, notably the US. There's a short article on some of these issues from 2010 here https://bit.ly/2Y318rL.

Which whistleblowing route should a whistleblower follow?

Under the EU whistleblowing rules, the choice of routes for making a report are as follows:

- Making an internal report within an organisation – as a rule of thumb this should be a whistleblowers' primary route of action but this route can be bypassed under certain circumstances;
- Making an external report to a relevant national authority – this can be undertaken under some circumstances, such as where the use of internal channels cannot reasonably be expected to function properly, in particular where a whistleblower has valid reasons to believe that they would suffer retaliation in connection with their whistleblowing, including as a result of a breach of confidentiality, or that the relevant authorities would be better placed to take effective action to address the reported breach;
- Making a report to the media – a whistleblower can only pursue this route of action either where no appropriate action was taken in response to the initial (internal) report at either the internal or external reporting stages, or, in cases of imminent danger to public interest, or (in the external reporting context) where there is a risk of retaliation or a low prospect of the breach being effectively addressed.

What does internal reporting mean?

EU countries must encourage reporting through internal reporting channels before reporting through external reporting channels, where the breach can be addressed effectively internally and where a whistleblower considers that there is no risk of retaliation.

Under the EU whistleblowing rules, EU countries are obliged to ensure that private and public sector organisations establish channels and procedures for internal reporting and for follow-up. Here "follow-up" means action taken (by a report recipient or relevant authority) to assess the accuracy of the allegations made in a report and, where relevant, to address the reported breach through appropriate means.

Internal reporting applies to private sector organisations with 50 workers or more, to which exceptions apply, notably financial services subject to EU money laundering and terrorist financing rules, and EU countries can also choose to not apply this threshold subject to making an appropriate risk assessment. Private sector organisations with 50 to 249 workers may share resources as regards the receipt of reports and any investigation to be carried out. Reporting channels may be operated internally by a person or department designated for that purpose or provided externally by a third party.

Procedures for internal reporting and follow-up must cover a number of things including the following:

- Channels for receiving reports which are secure and ensure that the confidentiality of the whistleblower and any third party mentioned in a report is protected – access by non-authorised staff members must also be prevented. Reporting can be made in writing or orally, or both; oral reporting must be possible by phone or through other voice messaging systems, and, if requested by a whistleblower, by means of a physical meeting within a reasonable timeframe;
- Acknowledgment of receipt of a report to the whistleblower within seven days of that receipt;
- The designation of an impartial person or department competent for following-up on reports which may be the same person or department as the one that receives the reports and which will maintain communication with the whistleblower and, where necessary, ask for further information from and provide feedback to that whistleblower – here 'feedback' means giving the whistleblower information on the action envisaged or taken as follow-up and about the grounds for the follow-up;
- Diligent follow-up by the designated person or department referred to immediately above, and diligent follow-up where provided for in national law as regards anonymous reporting;
- A reasonable timeframe to provide feedback, not exceeding three months from the acknowledgment of receipt or, if no acknowledgement was sent to a whistleblower, three months from the expiry of the seven-day period after the report was made; and,
- Providing clear and easily accessible information regarding the procedures for reporting externally to the relevant authorities.

What does external reporting mean?

Under the EU whistleblowing rules, without prejudice to making a public disclosure (see later below), whistleblowers report externally either after having first reported through internal reporting channels or by directly reporting through external reporting channels.

EU countries have to designate the relevant authorities who can receive, give feedback and follow up on whistleblowing reports and must ensure that these authorities do the following:

- Establish independent and autonomous external reporting channels to receive and handle information about breaches – these must meet certain criteria (as set out in the EU whistleblowing rules). These channels must enable reporting in writing and orally; oral reporting must be possible by phone or through other voice messaging systems and, upon request by the whistleblower, by means of a physical meeting within a reasonable timeframe;
- Promptly, and in any event within seven days of receiving a whistleblowing report, acknowledge receipt, unless a whistleblower has explicitly requested otherwise or the relevant authority reasonably believes that acknowledging receipt would jeopardise protecting the whistleblower's identity;
- Diligently follow up on the reports;
- Provide feedback to the whistleblower within a reasonable timeframe not exceeding three months, or six months where that is justified;
- Communicate to the whistleblower the final outcome of investigations triggered by the report, in accordance with national law procedures; and
- Transmit in due time the information contained in the report to the relevant EU institutions etc. for further investigation, where provided for under EU or national law.

EU countries may also provide other procedures for relevant authorities to use, for example concerning closing procedures for minor breaches or repeat reports. EU countries must also ensure that the relevant authorities designate staff members responsible for handling reports appropriately (as set out in the EU whistleblowing rules). EU countries must also ensure that the relevant authorities publish on their websites in a separate, easily identifiable and accessible section certain information, for example the procedures applicable to the reporting of breaches, including the manner in which the relevant authorities may request a whistleblower to clarify the information reported or to provide additional information, the timeframe for providing feedback and the type and content of that feedback.

What does public disclosure mean?

A person who makes a public disclosure qualifies for protection under the EU whistleblowing rules if any of the following conditions is fulfilled:

1. The whistleblower first reported internally and externally, or directly externally in accordance with the applicable internal and external rules, but no appropriate action was taken in response to the report within the applicable internal or external reporting timeframes; or
2. The whistleblower has reasonable grounds to believe that: (i) the breach may constitute an imminent or manifest danger to the public interest, such as where there is an emergency situation or a risk of irreversible damage; or, (ii) in the case of external reporting, there is a risk of retaliation or there is a low prospect of the breach being effectively addressed, due to the particular circumstances of the case, such as those where evidence may be concealed or destroyed or where a relevant authority may be in collusion with the perpetrator of the breach or involved in the breach.

The above doesn't however apply to cases where an individual directly discloses information to the press pursuant to specific national provisions establishing a system of protection relating to freedom of expression and information.

Can a whistleblowers' identity be disclosed (duty of confidentiality)?

No – only exceptionally. For both internal and external reporting, a whistleblower's identity must not be disclosed to anyone apart from staff members authorised to receive or follow up on reports, without the explicit consent of the whistleblower. This also applies to any other information from which the whistleblower's identity may be directly or indirectly deduced. As an exception to this, the identity of a whistleblower may be disclosed where there is a necessary and proportionate obligation imposed by EU or national law in the context of investigations by national authorities or judicial proceedings.

Does the EU General Data Protection Regulation (GDPR) apply?

Yes. For both internal and external reporting. Any processing of personal data carried out pursuant to the EU whistleblowing rules, including the exchange or transmission of personal data by authorities, must be done in compliance with GDPR. There is some background to GDPR here www.bit.ly/gdprfaq.

Personal data which are manifestly not relevant for the handling of a specific whistleblowing report must not be collected – if they are accidentally collected they must be deleted without undue delay.

Are there any record-keeping obligations?

Yes, for both internal and external reporting – these are very prescriptive. EU countries must ensure that organisations in the private and public sectors and the relevant authorities keep records of every whistleblowing report received. In order to be compliant, reports must be stored for no longer than is necessary and proportionate. GDPR will again be a consideration here. Note that previously some Data Protection Authorities have suggested retention periods should be short – for example CNIL in France previously suggested a two month retention period after a report had been dealt with.

Where a recorded phone or other recorded voice messaging system is used for reporting, subject to the consent of the whistleblower and any other local law requirements, organisations in the private and public sectors and the relevant authorities can document the oral reporting in one of the following ways:

1. By making a recording of the conversation in a durable and retrievable form; or
2. Through a complete and accurate transcript of the conversation prepared by the staff members responsible for handling the report.

The whistleblower must be offered the opportunity to check, rectify and agree the transcript of the call by signing it.

Where an unrecorded phone or other unrecorded voice messaging system is used for reporting, organisations in the private and public sectors and the relevant authorities can document the oral reporting in the form of accurate minutes of the conversation written by the staff member responsible for handling the report. The whistleblower must be offered the opportunity to check, rectify and agree the minutes of the conversation by signing them. This will be an important consideration for those companies who outsource their whistleblowing helpline – you will likely want to include a contractual provision with your helpline provider that they will keep records to enable you to comply with your legal obligations.

Where a person requests a meeting with the staff members of organisations in the private and public sectors or the relevant authorities for whistleblowing purposes organisations in the private and public sectors and relevant authorities must ensure, subject to the consent of the whistleblower, that complete and accurate records of the meeting are kept in a durable and retrievable form. Organisations in the private and public sectors and the relevant authorities can document the meeting in one of the following ways:

1. By making a recording of the conversation in a durable and retrievable form; or
2. Through accurate minutes of the meeting prepared by the staff members responsible for handling the report.

The whistleblower must be offered the opportunity to check, rectify and agree the minutes of the meeting by signing them.

Is retaliation prohibited?

Yes, for all types of organisation – the forms of prohibited retaliation are quite extensive. Here 'retaliation' means any direct or indirect act or omission which occurs in a work-related context, is prompted by internal or external reporting or by public disclosure, and which causes or may cause unjustified detriment to the whistleblower.

Necessary measures to prohibit any form of retaliation against whistleblowers must be put in place by EU countries. Retaliation includes threats of retaliation and attempts at retaliation including the following (which are non-exhaustive):

- Suspension, lay-off, dismissal or equivalent measures;
- Demotion or withholding of promotion;
- Transfer of duties, change of location of place of work, reduction in wages, change in working hours;
- Withholding of training;
- A negative performance assessment or employment reference;
- Imposition or administering of any disciplinary measure, reprimand or other penalty, including a financial penalty;
- Coercion, intimidation, harassment or ostracism;
- Discrimination, disadvantageous or unfair treatment;
- Failure to convert a temporary employment contract into a permanent one, where the worker had legitimate expectations that they would be offered permanent employment;
- Failure to renew, or early termination of, a temporary employment contract;
- Harm, including to the person's reputation, particularly in social media, or financial loss, including loss of business and loss of income;
- Using blocking lists on the basis of a sector or industry-wide informal or formal agreement, which may entail that the person will not, in the future, find employment in the sector or industry;
- Early termination or cancellation of a contract for goods or services;
- Cancellation of a licence or permit; and
- Psychiatric or medical referrals.

The EU whistleblowing rules set out a number of necessary measures that EU countries must put in place concerning retaliation against whistleblowers including providing for remedies and compensation.

Also, where whistleblowers report information on breaches or make a public disclosure in accordance with the EU

whistleblowing rules they won't be considered to have breached any restriction on disclosure of information and won't incur liability of any kind in respect of a report or public disclosure, so long as they had reasonable grounds to believe that the reporting or public disclosure of the information was necessary for revealing a breach pursuant to the EU whistleblowing rules.

Further, whistleblowers will not incur liability in respect of the acquisition of or access to the information which is reported or publicly disclosed, so long as this acquisition or access did not constitute a so-called 'self-standing criminal offence'. In the event of the acquisition or access constituting a 'self-standing criminal offence' criminal liability is governed by national law (for example under s.170 of the UK Data Protection Act 2018).

Finally, in legal proceedings, including for defamation, breach of copyright, breach of secrecy, breach of data protection rules, disclosure of trade secrets, or for compensation claims based on private, public, or on collective employment law, whistleblowers will not incur liability of any kind as a result of reports or public disclosures under the EU whistleblowing rules.

Are individuals subject to whistleblowing allegations also protected?

Individuals to whom breaches of relevant EU law are attributed to or associated with under whistleblowing have full legal rights including the right to a fair trial, the presumption of innocence, the right to be heard and the right to access their file etc. Their identities must also be protected for as long as investigations triggered by a whistleblowing report or public disclosure are ongoing.

What penalties apply?

It is at the discretion of EU countries to provide for penalties under their national law, which must be effective, proportionate and dissuasive, with regard to:

- Hindering or attempting to hinder whistleblowing;
- Retaliation against whistleblowers;
- Bringing vexatious proceedings against whistleblowers; and
- Breaching the duty of maintaining the confidentiality of the identity of whistleblowers.

What about false whistleblowing?

EU countries have to provide penalties for where whistleblowers have knowingly reported or publicly disclosed false information, and also provide for measures to compensate for damage resulting from such reporting or public disclosures.

Can whistleblowing rights and remedies be waived?

EU countries must ensure that rights and remedies under the EU whistleblowing rules cannot be waived or limited by any agreement, policy, form or condition of employment, including a pre-dispute arbitration agreement.

When must the EU whistleblowing rules be implemented?

EU countries have to implement the EU whistleblowing rules into national law by 17 December 2021.

By way of derogation to this date, as regards organisations in the private sector with 50 to 249 workers, EU countries must implement the obligation to establish internal reporting channels by 17 December 2023.

What about the UK and Brexit?

The UK government has stated that due to Brexit the UK will not be implementing the EU whistleblowing rules. But, generally-speaking, existing UK whistleblowing rules largely reflect the EU whistleblowing rules, at least in terms of general underlying principles.

What are the key takeaways?

Each EU country must implement the whistleblower rules into national law. For those EU countries that have only partial existing whistleblower rules this will be a major task as the EU whistleblowing rules are quite extensive. Not all EU countries have a good record of implementing EU law to meet EU deadlines either, so there may be delays. Most significantly, the EU whistleblowing rules allow EU countries plenty of implementing discretion – this will likely lead to plenty of local variations (and not just for penalties and anonymity – the EU whistleblowing rules allow for EU countries to give whistleblowers more favourable rights than in the EU whistleblowing rules). All told, setting up an EU-wide whistleblowing compliance programme will be challenging.

Does whistleblowing present any data protection issues?

Yes. Typically stock exchange listed businesses (especially in the US) adopt compliance systems across their corporate group that provide whistleblowing helplines etc. for their employees – employees are often required to report suspicious behaviour. However, pre-GDPR, this often fell foul of data protection rules in a number of European countries, notably France. Note that France has also adopted anti-corruption legislation, the so-called Sapin II law (see http://bit.ly/sapinlaw), which has also brought about additional regulatory whistleblowing requirements.

The data protection regulators of some European countries have required regulatory approval to be given before personal data can be collected and processed under a whistleblowing scheme – often certain conditions must be satisfied. The UK's data protection regulator does not require approval of a helpline in itself although it may be necessary to register data processing with the ICO and pay an annual fee (see https://www.corderycompliance.com/solutions/privacy-registration-and-renewal/).

The CNIL and other data protection regulators, including in Germany, and have also made it clear that, in their view, whistleblowing services are considered as high risk data processing and must therefore be subject to a Data Protection Impact Assessment.

GDPR has empowered individuals with lots of rights. A key issue here is that some of these rights may conflict with protecting whistleblowers against the risk of retaliation for whistleblowing.

Perhaps the key area concerns Subject Access Requests (SARs). For example, where an employee provides information about another employee to an employer and the latter employee afterwards makes a SAR, this latter employee can gain access to their personal data, including (under Article 15(1)(g)) "where the personal data are not collected from the data subject, any information as to their source". The consequence could be that this would reveal the whistleblower's identity. It may be that they best way to deal with this is to redact all the whistleblower's personal data from a given document, or, if this can't be done practicably, the alternative may be to withhold the disclosure of the whistleblower's personal data on the grounds that this would interfere with their rights and freedoms. These may be difficult decisions to make and it is likely that specialist advice will be needed to help balance conflicting rights and obligations.

Another issue is determining what the appropriate legal basis should be for processing personal data in whistleblowing situations. It will be recalled that the general conditions for processing data are set out under GDPR Article 6 and under GDPR Article 9 for special categories of personal data. The EU WP29 (now effectively replaced by the European Data Protection Board) examined this issue under the pre-GDPR rules in "WP 117: Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime". Here, WP29 took the view that potentially there were two lawful grounds for processing personal data (in the particular whistleblowing contexts that it was looking at), namely: (i) the processing is necessary for compliance with a legal obligation to which the data controller is subject; and, (ii) the processing is necessary for the purposes of the legitimate interests pursued by the data controller or parties to whom the data are disclosed. WP29's view was that the first ground could apply in certain contexts such as banking where the EU had provided for internal control legal compliance obligations, but it ruled out this ground where foreign law had imposed a legal obligation on the basis that this would make it easy for foreign rules to circumvent the then existing EU data protection rules (and so US SOX

whistleblowing helplines could not be legitimised on this legal basis).

As regards the second ground, WP29's view was that this could potentially be relied on as there was a "legitimate interest" in ensuring the stability of financial markets and preventing fraud, bribery and financial crime; this did however require a balance to be struck between a "legitimate interest" and an individual's fundamental rights. These two legal grounds for processing are similar under GDPR (although the "legitimate interests" grounds has had some changes made to it) so WP29's guidance could also be followed under GDPR. It is important to remember thought that the WP29 guidance is just guidance – ultimately these matters will be settled by the courts. If the "legitimate interests" ground were to be pursued a "legitimate interests assessment" should be undertaken.

What should we do now?

Businesses can consider doing the following:

1. Make sure that you review your whistleblower policies. You may want counsel experienced in this area to help you. Check that it your policy is not too restricted. Is it clear that matters such as competition law, data protection, environmental and product liability are in scope?

1. Review your internal procedures. Again you may want specialist counsel to help. Are you clear on your revised processes? Can your team determine what's covered by the Directive? Will a flowchart or chronological list help? How can you be sure you'll meet the deadlines for acknowledgement, substantial determination, retention etc.?
2. Choose any helpline provider wisely. Some are better than others. You will need a provider who understands GDPR issues, passes your due diligence tests and is able to enter into a contract with appropriate safeguards and penalties if they get it wrong. You're also likely to need their help with your compliance obligations e.g. recording contact so make sure that's covered in your contract too;
3. Explain to employees the scope of your helpline and how it should be used – keep it straightforward and simple so as to not discourage whistleblowing. Make sure you comply with your GDPR transparency obligations;
4. Recommend to employees that if they use a whistleblowing helpline they should supply any personal data about themselves confidentially. Where practical consider discouraging employees from naming individuals when making whistleblowing disclosures – this may of course prove impossible;
5. When processing personal data supplied by a whistleblower limit it to what is necessary to be able to handle an investigation. From our experience whistleblowers often try to pass on information that is irrelevant to the whistleblowing allegations – this information should likely be restricted or deleted so that only personal data which is strictly needed for the investigation is passed on to the investigators;
6. Ensure that employees accused of wrongdoing through whistleblowing are informed promptly about this except in some limited circumstances;
7. Ensure that personal data obtained through a whistleblowing disclosure is retained securely and protected against loss, theft, damage etc.;
8. Ensure that any necessary data transfers outside the EU/EEA or UK of personal data obtained through a whistleblowing disclosure are lawful e.g. by using EU Standard Contractual Clauses – depending on the circumstances it may be best to not transfer the data at all;
9. Strictly limit the time for which data obtained through a helpline is retained. Also limit the time for which the personal data obtained through a whistleblowing disclosure is held;
10. Comply with any notification or consultation requirements with data protection regulators or Works Councils;
11. Review your communications with employees and others about whistleblowing. Do wallet cards, posters and other collateral need to be changed? Again you'll need also to make sure you comply with your GDPR transparency obligations;
12. Train relevant staff on all of the above;
13. Undertake regular compliance reviews or audits to identify and rectify issues; and
14. Keep abreast of changes in the law. As we have said local law across the EU is likely to vary and you'll need to make sure that you comply in each jurisdiction where you do business or employ people.

More information

Cordery's GDPR Navigator includes resources to help deal with data protection compliance. GDPR Navigator includes:

- Detailed guidance on the core principles of GDPR in paper and on film;
- Guidance on due diligence;
- Guidance on data retention; and,
- A monthly call to look at GDPR enforcement throughout the EU & the UK.

We report about data protection issues here: http://www.corderycompliance.com/category/data-protection-privacy/. For more about GDPR please also see our GDPR FAQs which can be found here: http://www.corderycompliance.com/eu-data-protection-regulation-faqs-3/ and our Data Protection Glossary which can be found here: http://www.corderycompliance.com/?s=glossary.

The EU law can be found here: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32019L1937

For more information please contact André Bywater or Jonathan Armstrong who are lawyers with Cordery in London where their focus is on compliance issues.

Jonathan Armstrong, Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH
Office: +44 (0)207 075 1784
Jonathan.armstrong@corderycompliance.com

André Bywater, Cordery, Lexis House, 30 Farringd Street, London, EC4A 4HH
Office: +44 (0)207 075 1785
Andre.bywater@corderycompliance.com