EU Whistleblowing Rules – Are You Ready?

Date : November 12, 2021

Introduction

The 17 December 2021 deadline for implementation of the EU whistleblowing directive ("the EU rules") is fast approaching. To date only two EU countries have actually implemented, some may make it just in time, and others will miss the deadline and be late in their implementation. Whilst this may present some challenges for your business depending on where you're located, this doesn't mean that you shouldn't be in some state of advanced readiness – there's plenty to be done and gaps can be filled in later.

What are the top dozen or so things you need to know about the EU rules?

- **Scope** – the EU rules cover a wide number of areas of EU law and whilst some areas will only affect some businesses other areas will affect all businesses e.g. competition/antitrust. Also, it looks like some EU countries are going to include other areas that individuals can speak up about. Make sure you know what's in scope for your business;
- **Who is a whistleblower** – individuals who can be considered as whistleblowers under the EU rules include not just employees but the self-employed and those who've left the business. Make sure everyone in your business is aware of who can speak up;
- **Reporting routes** – reporting can be done internally (the preferred route under the EU rules), externally to a regulator/authority, or to the public. Make sure your business promotes the internal route;
- **Procedures** – reporting channels and follow-up must be established to handle whistleblowing claims, where strict deadlines apply. Make sure your business has clear and understandable processes in place;
- **Record-keeping obligations** – records must be kept and observe certain formalities. Make sure your business keeps records diligently – there's quite a bit to do;
- **Hotlines** – reporting channels may be provided externally by a third party. If your business uses an external hotline make sure the service provider has made the changes to adapt to the EU rules;
- **Confidentiality** – a whistle-blower's identity must be kept confidential. Ensure that your business gets this message across to those who may be considering speaking up as they need to feel confident about this;
- **Anonymity** – it is up to each EU country to decide on whether to allow for anonymous reporting or not and if so under what conditions. Where applicable, make sure that your business deals with anonymity appropriately;
- **Data protection** – many data protection issues need to be addressed, for example, irrelevant data must not be collected and if they are accidentally collected they must be deleted quickly, and Subject Access Requests may need to be addressed. It is well worth the business putting time and resources into this – don't get caught out by data protection compliance in speaking up cases;
- **Retaliation** – retaliation against whistle-blowers is strictly prohibited. Retaliation comes in many possible forms and may prove a challenge for businesses to handle. Businesses must get the message across their organization about zero tolerance for retaliation (or otherwise risk facing challenging legal battles down the line);
- **The accused** – individuals subject to whistleblowing allegations are also protected. Make sure your business observes the innocent until proved guilty principle;
- **False whistleblowing** – those who knowingly report or publicly disclose false information may be subject to sanctions. Businesses must be able to spot and swiftly deal with any false speaking up; and,
- **Waiver** – whistleblowing rights and remedies cannot be waived. Businesses will need to ensure that they observe speaking up right and remedies.

What are the top half a dozen things that I can do?

Businesses should consider doing the following key things:

- Update/introduce the relevant documentation including a whistleblowing policy and an internal manual for the team handling whistleblowing matters;

- Ensure that internal procedures and policies are in place to protect a whistleblower's identity and the contents of a whistleblowing disclosure;
- Ensure that no retaliation against a whistle-blower takes place;
- Address data protection issues including ensuring that: you have undertaken a Data Protection Impact Assessment; personal data obtained through a whistleblowing disclosure is retained securely and protected against loss, theft and damage; and, any necessary data transfers outside the EU/EEA of personal data obtained through a whistleblowing disclosure are lawful e.g. by using the *new* EU Model Clauses(but also consider whether you need to transfer personal data at all);
- Comply with any notification requirements to data protection regulators or Works Councils; and,
- Train relevant staff on all of the above.

Please refer to our FAQs and film for more details about the above here https://www.corderycompliance.com/eu-whistleblowing-faqs-2/.

A recent podcast that we did about whistleblowing can be found here https://www.corderycompliance.com/life-with-gdpr-eu-whistleblower-directive-part1/ and other articles that we've written about whistleblowing can be found here https://www.corderycompliance.com/uk-whistleblowing-speaking-up/ and here https://www.corderycompliance.com/lux-whistleblowing-echr-judgement/.

The EU whistleblowing directive 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