

VISCHER

EU Whistleblower Directive.

The impact on multinational companies
– with a focus on data privacy

David Rosenthal
May 25, 2021

Whistleblowing Hotlines

- It all began with Sarbanes-Oxley in 2002 ...
- Today such hotlines are a well accepted compliance tool
- EU Whistleblower Directive increased the pressure
 - Private companies in the EU with 50+ employees must have own internal reporting channels; companies with fewer than 250 employees can share them with affiliates (and have more time)
 - Directive must be implemented in national law by December 17, 2021
 - Main focus is the protection of whistleblowers
 - They are allowed to directly report externally
 - Only violation of Union law (Annex, 10 pages) is in scope, but member states can go further

Draft bill in Germany also covers German law and provides for fines up to EUR 100'000

26.11.2019 EN Official Journal of the European Union L 305/17

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 Union law

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,
Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16, Article 43(2), Article 50, Article 53(1), Articles 91, 100, and 114, Article 168(4), Article 169, Article 192(1) and Article 325(4) thereof and to the Treaty establishing the European Atomic Energy Community, and in particular Article 31 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the Court of Auditors (1),

Having regard to the opinion of the European Economic and Social Committee (2),

After consulting the Committee of the Regions,

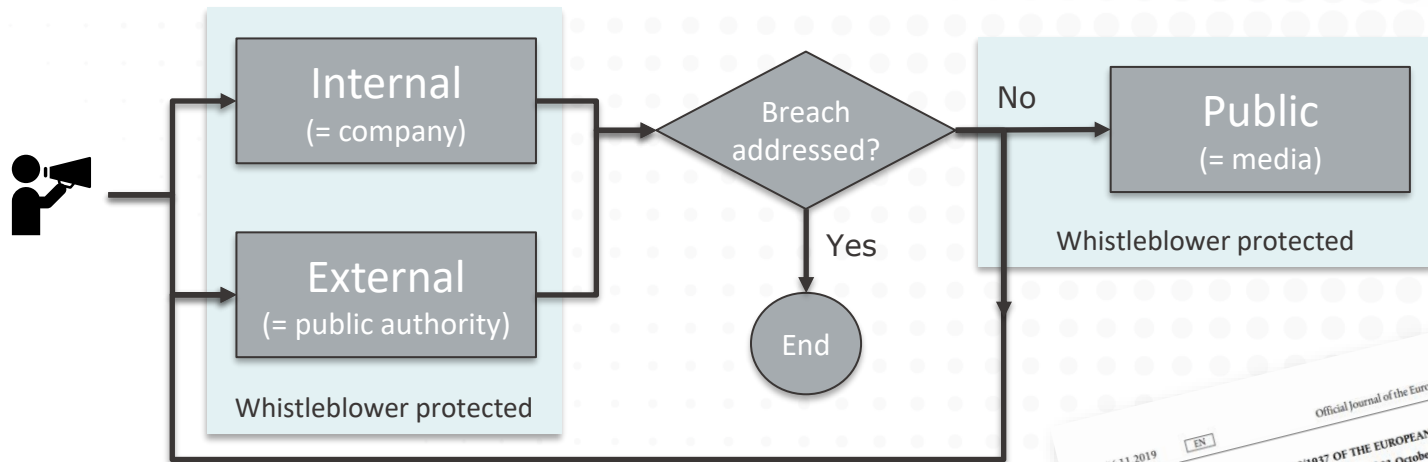
After consulting the opinion of the Group of Experts referred to in Article 31 of the Treaty on the Functioning of the European Union,

Have (1),

in the con-

Three Tier Reporting

Incentive to have a good process



Persons making a public disclosure should qualify for protection in cases where, despite internal and external reporting, the breach remains unaddressed, for instance in cases where the breach was not appropriately assessed or investigated, or no appropriate remedial action was taken. The appropriateness of the follow-up should be assessed according to objective criteria, linked to the obligation of the competent authorities to assess

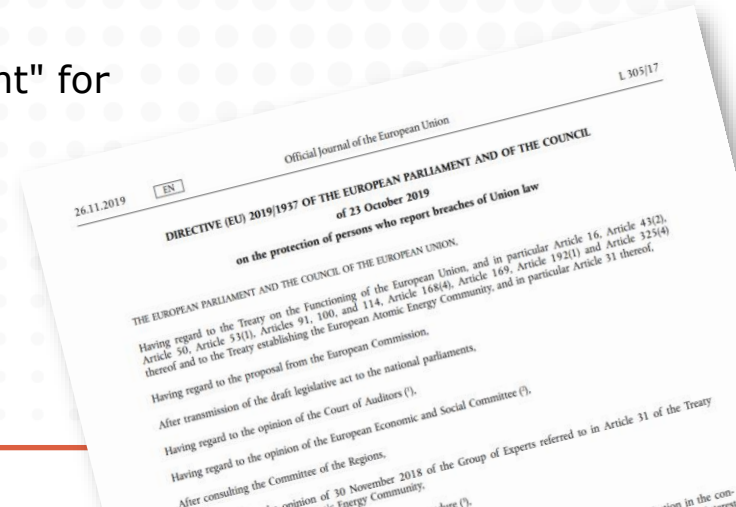
Recital 79

26.11.2019 EN
Official Journal of the European Union
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 Union law

in particular Article 16, Article 43(2),
Article 192(1) and Article 325(4)
of the Treaty on the Functioning of the European Union,
Having regard to the draft legislative proposal,
After transmission of the draft legislative proposal to the Economic and Social Committee (ESC),
Having regard to the opinion of the Court of Auditors (COA),
Having regard to the opinion of the European Economic and Social Committee (EESC),
Having regard to the opinion of the Committee of the Regions (CoR),
After consulting the Committee of the Regions,
After consulting the opinion of 30 November 2018 of the Group of Experts referred to in Article 31 of the Treaty
on the Functioning of the European Union,
here (),

Directive sets minimum standards

- Requirements for companies (Art. 9)
 - Reports shall be possible in writing or orally (i.e. telephone or "other voice messaging" and, upon request, physically)
 - Transcripts and meeting minutes can be checked by the reporter
 - Reporting should be possible not only by employees (e.g., job candidates, advisors)
 - Designation of an "impartial person or department" for following up on reports
 - Report must be confirmed within seven days
 - Diligent "follow-up" on reports
 - Feedback to whistleblower within three months
 - Information on how to report externally



Some Pitfalls for Multinationals

- Pitfall 1: Legal entity view
 - Sharing of resources only for entities with <250 employees
 - Solution: Contract with provider and internal segregation
- Pitfall 2: Country-specific implementation
 - Differences in scope, requirements and reporting authorities
 - Solution: Gold standard as a minimum standard, country-specific follow-up information to reporters
- Pitfall 3: Reports to entities that are *not* subject to the Directive
 - Solution: Voluntary protection, potentially with exceptions
- Anonymity, Data Protection → next slides

Anonymity?

- Remains a hot topic, even under the Directive
- Anonymous reports permitted under the Directive
- Confidentiality of reporting person needs to be "safeguarded", but no absolute protection

Safeguarding the confidentiality of the identity of the reporting person during the reporting process and investigations triggered by the report is an essential *ex-ante* measure to prevent retaliation. It should only be possible to disclose the identity of the reporting person where that is a necessary and proportionate obligation under Union or national law in the context of investigations by authorities or judicial proceedings, in particular to safeguard the rights of defence of persons concerned. Such an obligation could derive, in particular, from Directive 2012/13/EU of the European Parliament and of the Council⁽⁴²⁾. The protection of confidentiality

Recital 82

- Germany: No obligation to follow-up on anonymous reports
- Do not promise confidentiality! Beware of what you put into the personnel file (cf. LAG BW December 20, 2018, 17 Sa 11/18)

Data Protection Issues – 1

Watch out also for local employment law issues

- GDPR and Swiss Data Protection Act apply
 - Personal data on both reporting and accused persons
 - Art. 18 of the Directive provides legal basis for records keeping
 - Joint controllership? If resources are shared, a contract is needed
 - Fines for breach of the GDPR are more threatening ...
- Basic principles apply
 - Principle of lawfulness
 - Principle of purpose limitation
 - Principle of data minimization
 - Principle of storage limitation
 - Technical and organizational measures of data security

Define scope of what may be reported

Data Protection Issues – 2

- Information obligations
 - Data subjects (reporters, accused, others) need to be provided with defined minimum information (Art. 13/14 GDPR)
 - General information not sufficient; inform also specifically asap
- Records of Processing Activities (ROPA)
 - Hotline/follow-up processing as a combined processing activity
- Data Protection Impact Assessment (DPIA)
 - Describe processing activity, assess possible negative consequences, discuss measures to mitigate/avoid them
 - Measures include a policy to govern handling of reports
 - Document DPIA, involve DPO (and work council)

Data Protection Issues – 3

- Right of access
 - Accused person (and others) has a right to access personal data
 - Includes sections of whistleblowing or investigational reports insofar related to the data subject
 - Balancing of interests: Whistleblower vs. accused person
 - Not to confuse: Employee's right to be heard and of due process
- Retention of documents
 - Personal data may only be stored for as long as needed and suitable in order to comply with legal obligations
 - When to delete or anonymize personal data?
 - How to mitigate risk of later accusations or regulatory inquiries?

Retention Periods


- Data Protection Authorities push for (unrealistic) short periods
 - No retention if case unsubstantiated
 - Within two months of completion of the investigation
- Not considered by them: Legal and regulatory action
 - Legal claims may be raised (3-10 years)
 - Company may wish to prove proper handling (2-10 years)
- Not considered by them: Employment law requirements
 - Retention as evidence, e.g., for reference letter (duration of employment + 5-10 years) or in case of retaliation (80% of retaliation occurs within three weeks of a report, 90% within six months)

Data Protection Issues – 4

- Right of erasure
 - Erasure can be requested by any data subject
 - Request can be refused as long as personal data is still needed for pursuing a legal action or complying with a legal obligation
- Right of rectification
 - Only insofar personal data is incorrect in view of its purpose
- Cross-border / delegated processing
 - Ideally, data is kept in Europe – beware of "Schrems II" when using the cloud or a US-based whistleblowing hotline
 - Enter into "Data Processing Agreements" with service providers
 - Share Group hotlines: Enter into intra-group agreements

Three Steps

1. Regulate whistleblowing and inform people about it
 - What can be reported, by whom and where
 - What happens with reports (processes, responsibilities)
 - Protection of whistleblowers *and* of accused persons
 - Rights of individuals (data protection, employment law)
2. Implement channels and case management resources
 - Ensure proper data security and retention policies
 - Contract with internal/external operator of the "hotline"
3. Perform data protection governance tasks
 - ROPA, DPIA, transfer risk assessment, works council



If unsure, use German law as a gold standard

Soon to be released:
ISO 37002 Guidance
on Whistleblowing
Management Systems

VISCHER

And now let's discuss!

Questions? drosenthal@vischer.com

Zürich

Schützengasse 1
Postfach
8021 Zürich, Schweiz
T +41 58 211 34 00

www.vischer.com

Basel

Aeschenvorstadt 4
Postfach
4010 Basel, Schweiz
T +41 58 211 33 00

Genf

Rue du Cloître 2-4
Postfach
1211 Genf 3, Schweiz
T +41 58 211 35 00



Free handbook on
internal investigations
to be released this
week (in German)

www.vischer.com/investigations