

**Whistleblower scheme – Article 30 record**

 Last updated XXXX – 2022

Pursuant to article 30 of the General Data Protection Regulation (hereinafter “GDPR”), a record must be maintained of the processing of personal data in the organisation's whistleblower scheme. Here is an example of how a record can be designed.

Data controller (Enter information about the organisation):

Contact:

E- mail:

Phone:

The purpose is to make a whistleblower scheme available to the organisation's staff in

accordance with the organisation's duties under the Whistleblower Directive and

[insert national legislation implementing the Directive].

Basis for processing personal data:

* GDPR Article 6(1), point c (necessary for compliance with a legal obligation, cf. article 8 of the Whistleblower Directive and [insert national legislation implementing the Directive]).

Exception to the prohibition on the processing of sensitive personal data and

information on criminal convictions and offenses:

* GDPR Article 9(2), point g (necessary for reasons of substantial public interest, cf. Article 8 of the Whistleblower Directive and [insert national legislation implementing the Directive]).
* GDPR Article 10 (legal basis in Article 8 of the Whistleblower Directive and [insert national legislation implementing the Directive]).

NOTE – if the organisation is not obliged under the Whistleblower Directive (if the

organisation has fewer than 50 employees) or national legislation, a different legal

basis for processing must be found. The following are possible legal bases for

processing:

[Basis for processing personal data:

* GDPR Article 6(1), point f (the legitimate interests rule) in that the organisation has a substantive interest in processing in-formation reported via a whistleblower scheme and this interest is deemed to carry more weight than the consideration for data subjects who may be mentioned in a report.

Exception to the prohibition on the processing of sensitive personal data and

information on criminal convictions and offenses:

* GDPR Article 9(2), point f (necessary for the establishment, exercise or defence of legal claims).
* GDPR Article 9(2), point g (necessary for reasons of substantial public interest).
* [insert national legislation implementing GDPR Article 10]].

**Categorising of data subjects**

* Employees
* Any whistleblowers who are not employees
* Persons who are the subject of a report
* Other partners, board members, etc.

**Categorising of personal data**

The information the whistleblower chooses to report to the whistle-blower scheme.

The whistleblower can choose to remain anonymous in connection with a report. The whistleblower may, however, choose to waive anonymity during the process, and a report concerning other identifiable persons will be considered processing covered by the data protection legislation.

**Special categories of information**

The processing may include specific categories of personal data pursuant to Article 9 of GDPR, if such data is covered by the report.

**Processing activities**

* Receive and screen reporting
* Assert impartiality
* Assess report
* Possible report to authorities
* Feedback to the whistleblower

**Where does the processing take place?**

The processing takes place on the premises of the organisation [and of the organisation's external advisor Whistleblower Partners, which manages the whistleblower scheme].

The processing takes place in operational centres located in the EU.

**Data processors**

Whistleblower Partners and its subprocessors in the EU.

The organisation's own internal IT systems.

**Recipients of personal data (independent data controllers)**

**Authorities**

If the inquiry gives rise to a report to an authority, the authority to which the report is made depends on the specific inquiry.

**Transfer to 3rd countries and international organisations**

Data is not transferred to countries outside the EU, nor to international organisations.

**Erasure**

The storage period depends on the specific case and what measures the case gives rise to. The information is erased as soon as it is no longer relevant in relation to documentation requirements vis-à-vis authorities, possible employment law disputes, etc.

Information covered by an unfounded report will be erased within [90 days] of the final assessment.

**Security measures**

An access and user management system has been established for the IT system that the data processor uses for the whistleblower scheme, and the system also features encryption and ensures anonymity.

With regard to the organisation's internal handling of information covered by a report, an access and user management system has also been established to ensure that only selected key employees have access to the information.