société d'avocats

nomosnetcom.fr **September 2017**

Whistleblowing: extension of the CNIL's Single Authorization

[DATA PROTECTION]
Deliberation n°2017-191 of 22 June 2017 modifying deliberation n°2005-308 of 8 December 2005 on the single authorization of data processing in the context of whistleblowing schemes

Following the adoption of the so called "Sapin II" Act of 9 December 2016 on the fight against corruption, which instituted common rules applying to whistleblowing schemes, the CNIL recently updated its Single Authorization relating to whistleblowing data processing.

The Single Authorization permits companies who wish to implement whistleblowing schemes to self-certify that their data processing comply with the CNIL's requirements set out under said Authorization. This allows them to avoid filing a formal request to obtain the CNIL's prior approval, which can be a long process.

The main modifications are as follows:

➢ **Extension of concerned whistleblowers**: the Authorization now covers whistleblowing schemes implemented for use not only by members of personnel, but also by external or occasional collaborators.

➢ **Broadening of purposes pursued by the data controller**: under the modified Single Authorization, processing are deemed compliant when the processed alerts are in relation to:

- A crime or an offence;
- A gross and manifest violation of laws or regulations, or of an act adopted by an international organization on the grounds of a ratified international commitment;
- A serious threat or damage to the general interest, of which the whistleblower has had personal knowledge;
- Reports relating to obligations defined under EU regulations, the French monetary and financial code or the French financial markets authority;
- Reports relating to the existence of behavior or situations that are contrary to the company's code of conduct, in respect of corruption or trading in influence facts.

The Authorization specifies that an alert may not include any elements protected by national defense secrecy, medical secrecy and/or attorney-client privilege.

➢ **Update of confidentiality rules regarding identity of data subjects**: as required by the Sapin II Act, elements permitting to identify whistleblowers may only be disclosed to the judicial authorities, and subject to the whistleblower's consent. Likewise, elements permitting to identify the person about whom the alert is made may only be disclosed to the judicial authorities and only once the alert is considered well-founded.

- **Specifications regarding data recipients**: alerts are now to be addressed to the direct or indirect supervisor, the employer or to the referent designated by the employer whereas the former Authorization used to more generally mention the persons specifically designated for this mission within the organization.

- **Strengthening of security measures**: it is reminded that the whistleblower's identity, and now also the identity of the persons about whom the alert is made and the information collected by all data recipients, are all to be treated confidentially.

- **Updating of information requirements**: the revised Authorization specifies that a clear and complete information of all potential users of the whistleblowing scheme shall be carried out, and delivered to the members of personnel but also to external and occasional collaborators (since those are now added to the list of potential whistleblowers).

  The Single Authorization also specifies, on the basis of the Sapin II Act, that the information shall detail the steps of the procedure implemented to collect alerts, in particular the recipients and the conditions under which they may receive an alert.

This revision thus mainly extends the scope of application of the Single Authorization. Those organizations who have already self-certified under the former Single Authorization do not need to self-certify again under the new version, but they shall double-check that their processing still meets the conditions set out under the new text in practice.

Camille BURKHART