Managing IT access and authorizations

In order to secure information systems (IS) and guarantee the confidentiality of the data they contain, authorization systems are becoming increasingly common in the workplace. This system ensures that **each** IS user can only access the data he or she needs to carry out his or her mission. Internally, this means setting up a mechanism for defining user authorization levels within the system, and a means of controlling data access permissions.

What is an authorization ?

Authorization is based on a pre-defined profile, generally linked to a **hierarchical position** or **function** within the organization, and not to a specific person.

This makes it easier to manage access in the event of staff movements. On the other hand, when accesses are allocated per person, you need to be extremely reactive and remove all accesses immediately if a member of staff leaves the department or structure.

The authorization must give each user the rights that are **strictly necessary for the performance of his or her duties**. In particular, it must determine:

- the data and applications to which the user may have dedicated or shared access (local or shared network, work files, printers, telephones, etc.);

- the extent of the rights granted: access for simple consultation, registration, deletion.

For what purposes can an employer set up an authorization system?

Personal data may be collected for **several purposes**, provided that these purposes are:

- **determined**;
- **explicit**;
- **legitimate**; and
- **not further processed** in a manner incompatible with these purposes

By virtue of this principle of **purpose limitation**, the APDP considers that the implementation of an authorization management system can meet the following objectives:

As part of the management of authorizations*:*

- to provide IS users with the technical and functional means to authenticate themselves to the information system so that they can carry out the functions and tasks for which they have been recruited;
- to manage changes in rights, internal transfers and departures;
- to update system accounts when administrative information changes (e.g. change of surname);
- to enable all account activation/deactivation/deletion tasks to be carried out;
- to carry out periodic control reviews to ensure that the rights issued comply with requests and the rules laid down in terms of access to information.

As part of the supervision of access to applications:

- to collect system events (logs) enabling user access to applications and data to be traced;
- to draw up alerts and/or reports to detect any risk of malicious intent and ensure that access is consistent with the authorizations issued;
- to establish evidence in the event of a dispute with any user (employee, service provider, etc.).

As part of anti-virus security:

- to set up alerts on intrusion risks;
- to draw up reports (e.g. security audit, risk detection, etc.).

What about the notion of surveillance or control?
An employer may decide to control or monitor the IT authorizations implemented within its entity. In this respect, the APDP considers that the notion of control or monitoring of the authorization management system should be understood as « *any activity consisting of the collection, detection and/or recording, within the framework of reports drawn up at regular intervals, of the personal data of one or more persons relating to the use of IT authorizations* ».

What justification is needed for the implementation of an authorization management system?

To be lawful, automated processing of personal data must meet at least one of the requirements set out in Article 5 of Law no. 1.565 of December 3, 2024.

The APDP thus considers that the implementation of an authorization management system can be justified by:

- ***Compliance with the data controller's legal obligations***

Certain data controllers are subject to specific obligations of **vigilance** and **traceability of transactions**. For banking or similar institutions, such obligations are set out in the following texts, among others:

- Law no. 1.338 of September 7, 2007 on financial activities and its implementing Sovereign Order;
- Law no. 1.362 of August 3, 2009 on the fight against money laundering, terrorist financing and corruption and its implementing Sovereign Order;
- Law no. 1.314 of June 29, 2006 relating to the carrying on of business as a custodian or administrator of financial instruments;
- Ministerial Order no 2012-199 of April 5, 2012 relating to the professional obligations of credit institutions acting as custody account-keepers for financial instruments.

The APDP believes that in order to comply with their obligations, these data controllers or their representatives may implement procedures for monitoring or controlling IT authorizations, in strict compliance with the principles defined by Law no. 1.565 of December 3, 2024, in particular the principles of **proportionality** and **transparency**.

- ***The fulfilment of a legitimate interest pursued by the data controller or a third party***

The APDP considers that a procedure for monitoring or controlling IT authorizations may also be justified by a **legitimate interest** of the data controller or a third party, such as:

- the optimization of the performance of its employees' work assignments;
- the security and proper technical operation of the computer network or system;
- the protection of the economic, commercial or financial interests of the data controller or its representative;

- the prevention and detection a priori and a posteriori of any non-compliant or illicit activity by users.

In view of the existence of **a subordinate or contractual relationship** between the employer and the employee, the latter's consent cannot constitute justification for the implementation of this type of processing.

What are the main principles governing IT authorizations?

- ***Authorization profiles defined, formalized and auditable***

Firstly, the APDP points out that for all categories of accounts (nominative or collective), it is necessary to identify and authenticate all users according to the level of risk associated with the resource, the type of user or the type of access. This separation of tasks and areas of responsibility means that access to personal data can be restricted to duly authorized users only.

In this respect, it requires compliance with both the « *need to know* » principle, which corresponds to the definition, by the business, of the authorizations required for a given user's activity, and the « *least privilege*» principle, which consists of implementing authorizations that are strictly necessary for the activities associated with each account.

The APDP also requests that the procedures for granting authorizations be documented.

It also points out that users' access permissions must be deleted or modified as soon as said users are no longer authorized to access a resource because they have left the entity or changed functions.

Finally, the APDP notes that it is imperative to ensure compliance with the rules for managing authorizations. The owners of the information system must regularly check the relevance of the profiles and access granted.

- ***A policy for validating authorizations and managing mobility***

The APDP insists on the fact that any request for authorization must be validated by at least the immediate superior of the authorized person. Furthermore, if the said superior delegates this task, he or she must nevertheless retain responsibility for the authorizations of his or her team and for those granted to people providing services on his or her behalf.

The APDP also asks the data controller to ensure that any change of post or departure is effectively managed in order to avoid an accumulation of authorizations. For example, when a person is transferred or leaves the entity, the authorizations held by that person must be modified or withdrawn immediately.

What information may be collected?

In accordance with the provisions of Article 4 of Law no. 1.565 of December 3, 2024, the collected personal data must be "*adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed* ".

The APDP therefore considers that only the following personal data may be collected and processed:

- identity : surname, first name and department of the employee, surname, first name and signature of the superior for the management of authorizations ;
- electronic identification data : identifiers of the authorized person (login and password);
- user account : account name, account domain, user group, type of rights ;
- connection data : logs, execution traces, time stamps, log files.

How long can data collected and processed as part of an authorization management system be kept?

The personal data collected **cannot be kept indefinitely** in a form that allows the data subjects to be identified.

The APDP therefore asks employers to provide for the following data retention periods:

- with regard to identity and user accounts: a maximum of 3 months after the employee has left the company;

- with regard to electronic identification data: for as long as the data subject uses the IS;

- with regard to connection data: a maximum of 1 year from the date of collection, depending on the activity carried out.

In any event, the APDP recommends, where possible, adopting a shorter retention period, once the data processed are no longer necessary to achieve the purpose(s) for which they were initially collected.

Finally, it points out that in the context of the initiation of legal proceedings, any necessary information resulting from the processing may be retained until the end of the said proceedings.

Who can access the data relating to authorizations?

Access to data relating to authorizations must be restricted to **only those people** who, as part of their job(s), can **legitimately be aware of them in view of the objectives of the system**.

For example, the IT department may have access to authorizations for the purposes of creating, modifying and deleting users and groups of profiles, and the AML manager may have access for the purposes of checking the authorization levels of the people in charge of anti-money laundering processing.

Similarly, an IT service provider may also have full rights for maintenance purposes. These access rights must then be limited to what is **strictly necessary for the performance of its service contract**. In addition, the service provider is subject to the same security and confidentiality obligations as those imposed on the data controller.

The APDP also considers that the communication of data to the Police Department (Direction de la Sûreté Publique) may be justified for the purposes of a judicial investigation.

In this respect, it points out that in the event of transmission, the aforementioned department may only have access to the information within the strict framework of its legally conferred missions.

Finally, the APDP considers that the Monegasque Financial Security Authority (Autorité Monégasque de Sécurité Financière or AMSF) and the Financial Activities Supervisory Commission (Commission de Contrôle des Activités Financières or CCAF) may, within the exclusive framework of the missions conferred upon them, be recipients of processed personal data.

How to inform data subjects?

It is imperative that all employers make users aware of their responsibility to protect their personal data.

In the interests of **transparency** towards users, as well as **fairness** in the collection and processing of personal data, the APDP therefore recommends that employers introduce a charter for the use of electronic communication tools, specifying, in particular when control or surveillance procedures are implemented:

- the purpose or purposes of these procedures;
- the persons authorized to have access to the data;

- how long the data collected will be kept;
- how data subjects may exercise their right of access to their data.

Finally, the APDP stresses the need to make all IS users aware not only of the authorizations granted to them and the resulting responsibilities, but also of the fact that all their actions are tracked.

What security measures should be put in place?

The APDP points out that the technical and organizational measures put in place to ensure the security and confidentiality of the processing with regard to the risks presented by the latter and the nature of the data to be protected must be maintained and updated, taking into account the state of the art, in order to maintain the high level of reliability expected throughout the period of operation of the processing.

It recommends that authentication should be carried out by means of an **identifier** and an **individual password that is deemed to be strong and regularly changed**.

In addition, access by authorized persons should be **logged**.

The APDP also requests that persons authorized to access the data processing be bound by a **particularly strict obligation of confidentiality**, specified in writing (for example in an IT charter, an administrator's charter or the employment contract).

Lastly, it accepts that data may be extracted and/or copied onto a separate medium for communication to legally authorized administrative or judicial authorities. In such cases, any copy or extraction of such data must be **encrypted on the receiving medium**.