L'ORÉAL LEGITIMATE INTERESTS ASSESSMENT (LIA) UNDER GDPR: IT devices Management

As part of L'Oréal legal obligation to document actions taken to comply with GDPR ("Accountability"), this questionnaire helps assessing whether legitimate interest(s)[1] can be used as a legal basis for the contemplated data processing activities.

This methodology assessment relies on the Guidelines of EU Data Protection Authorities.[2]

PRELIMINARY STEP

Methodology notes

Provide a description of the main data processing activities and purposes covered under this LIA

- **Main personal data processing activities:**

This LIA covers the processing of management of end-users IT devices (PCs, laptops, tablets, smartphones) used by L'Oréal employees and externals who works for L'Oréal (for example, external consultants) to execute their tasks in accordance with the contract signed with L'Oréal. This management is required by staff to execute their tasks with a device secured in accordance with L'Oréal IT security policy.

The only personal data processed is name, surname, civility/title, professional e-mail, and transactional data to ensure activities follow-up. This processing ensure communication with the end-user regarding IT devices accesses.

- **Purpose(s)covered:**

The purpose of this processing is the IT devices management of end-users to allow them to have access to a device from L'Oréal in order to execute their tasks.

STEP 1: ASSESSMENT OF THE OTHER LEGAL BASIS AVAILABLE

Methodology notes

If "YES" is selected for any of the questions of this section, it seems that instead of legitimate interests, the most appropriate legal basis would either be compliance with a law, contract or consent. In which case, skip Steps 2 to 4 and go straight to Step 5 to record this outcome.

Personal data can be used for different purposes, each of them having different legal basis., so answers to the questions below must clearly identify each purpose(s)for the personal data processing(s).

1.1 Are the personal data needed only to comply with a law or regulation? ~~YES~~ **NO**

If "YES" selected, please reference the legal provision under which personal data processing is necessary.

If "NO" selected, go to next question

1.2 Are the personal data only needed only to conclude or perform an agreement with the individuals? ~~YES~~ **NO**

[1] Per Art. 6) 1) f. GDPR

[2] See Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC and ICO Sample Legitimate Interest Assessment Template

If "YES" selected, consider whether there is an existing relationship with the individual (e.g. a contract, a transaction, a sale). In any case, please reference the existing or future agreement under which personal data processing are necessary.

If "NO" selected, go to next question

1.3 Is consent from the individuals only needed to process their personal data? ~~YES~~ **NO**

If "YES" selected, consider whether such consent is imposed by law (e.g. consent for cookies, digital marketing, consent for clinical studies), and reference such legal provision. When not imposed by law, consider whether it would still be possible to process the personal data without having consent of the individuals.

If "NO" selected, go to next section

STEP 2: IDENTIFYING A LEGITIMATE INTEREST(S) ("PURPOSE TEST")

Methodology notes

Explain how the legitimate interest(s) pursued are real (not speculative) and present (benefits are expected in a very near future). Give specifics and be clear enough (avoid vague or very general wording). "Interest(s)" refers to any objective or benefits pursued.

2.1 Identify if the interest(s) is pursued by L'Oréal (Group or entity) or by a third-party.

The interests are pursued by L'Oréal at Group and country levels.

2.2 Describe clearly and precisely what are the interest(s) pursued (e.g. direct marketing purposes, IT and network security, intragroup transfers for internal administrative purposes, fraud detection and prevention).

Interests pursued are both (i) internal administrative management to allow end-user access to devices they need to perform their tasks, and (ii) IT and network security as the devices provided are first set up in accordance with L'Oréal IT Security policies, to ensure devices used by end-users are secured properly.

2.3 Explain which benefits are expected from the processing and how important they are.

The benefits expected from such data collection are :

- The possibility for L'Oréal employees and externals who work for L'Oréal to give the means to perform their tasks;
- The ability to identify and contact employees and externals to keep them informed on their use of IT devices;
- To help keep tracks of which employee and externals is withholding which equipment ;
- To secure L'Oréal systems (by the follow-up of devices given) ;
- To ensure a minimum and homogeneous security level for L'Oréal networks and protect its sensitive assets (IT privacy policy).

That kind of benefits is important because necessary to the fulfilling of the requests.

2.4 Consider if such interest(s) benefit the individuals as well and how (e.g. processing adds specific value to the product/service to the individuals or adds protection to them).

The benefit for individuals (employees and externals) are:

- To have access to an IT device to perform their tasks;
- To be contacted by IT teams if they have an issue with their device.

2.5 Describe the impacts in case the processing could not take place (including any possible prejudice for L'Oréal, and for the individuals).

If the data processing could not take place, the impacts for L'Oréal would be:

- Loss of time, competences, talents or technologies for L'Oréal;
- Lack of competitiveness;

- Loss of market share and potential profits in the end;
- Inability for individuals to perform their tasks;
- Inability to protect L'Oréal systems;
- Inability to manage IT devices accesses;
- Inability to ensure follow-up of activities.

If the data processing could not take place, the impacts for individuals (employees and externals) would be:

- Inability to perform their tasks;
- Inability to access to L'Oréal networks with L'Oréal IT devices.

2.6 Identify if such interest(s) is triggered by the necessity to comply with a law/regulatory requirement (e.g. a foreign law with extraterritorial reach) or with industry guidelines, code of conducts or codes of practice.

These interests are not triggered by any specific law, regulatory requirement, industry guidelines, code of conducts. These interests are more triggered by best practices.

2.7 Identify if such interest(s) can raise any ethical issues/concerns.

None of ethical issues/concerns as very few personal data will be processed with no sensitive data.

2.8 Specify if a Data Protection Authority or a legal provision in data protection regulations already considered such interest(s) legitimate (e.g. Recital 47 GDPR referencing direct marketing). In which case, please reference it.

Yes – Recital 49 GDPR specifies that "The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned".

Also the CNIL's HR guide specifically mentions page 5 that managing employees access to networks and systems can be based on a legitimate interest.

STEP 3: IDENTIFYING THE NECESSITY FOR THE PURPOSE(S) PURSUED ("NECESSITY TEST")

Methodology notes
Provide detailed explanations about how the personal data processing are necessary to achieve the purposes.

3.1 Justify why all personal data collected are necessary to the purposes at stake.

The personal data collected regarding L'Oréal employees and externals are the following:

- Name, surname and civility/title to identify end-user regarding IT devices and to communicate with them;
- Civility/title allow to address the employee correctly;
- Professional e-mail to communicate with them;
- Transactional data (professional allocations (serial number of tools…) to ensure activities follow-up.

3.2 Consider if it would be possible to achieve the same purpose without processing the personal data (e.g. by anonymisation). In which case, describe how anonymization measures would be implemented. If not possible to proceed without personal data, explain why.

No – L'Oréal needs to be able to trace who are the employees receiving IT devices to be able to manage globally the equipment's (eg some do not need to have a professional mobile phone, only a professional laptop, other must have both).

3.3 Verify if there would be less intrusive way or means to process the personal data (e.g. by applying data minimization controls or pseudonymization measures). In which case, explain how such measures would be implemented.

No less intrusive measures identified considering the volume of personal data is already minimized to the strict necessary as follows: Contact details are necessary to reach an employee or an external, and the civility allows to address the person correctly. The professional e-mail allows to communicate with employees and externals about their IT devices (if needed).

The personal data are kept during the duration of the work's contract (for employees) and during duration of contract signed with L'Oréal (for externals). After the end of the contract, data is kept 3 years.

STEP 4: ASSESSING THE IMPACTS ON THE INDIVIDUALS' INTERESTS, RIGHTS, AND FREEDOMS

("BALANCING TEST")

Methodology notes
In this section, any impacts of the processing(s)on individuals' interests, rights and freedoms must be considered to assess if the legitimate interests pursued prevail over such individual's interests, rights and freedoms. Specific items need to be considered (e.g. sensitive nature of the data, reuse, information given, potential impacts on the individuals and their expectations) together with any additional safeguards.

Two outcomes are possible:

1. *There is no clear justification, or the outcome of the assessment is uncertain: it would be necessary to contemplate another legal basis (most probably consent)*
2. *There is a clear justification for the impact on the individuals: legitimate interests should be the appropriate legal basis*

Sensitive nature of the personal data – Vulnerable categories of individuals

4.1 Explain if any of the personal data qualify as "sensitive data" under Article 9 GDPR (e.g. biometrics, medical records, data revealing ethnic or origin, criminal records)

In this personal data processing, there is no personal data considered as "sensitive data" under Article 9 GDPR.

4.2 Explain if any of the personal data are likely to be perceived particularly private or intrusive by the individuals (e.g. credit card details, passport or national ID number, GPS location, salary, convictions/offences). Provide detailed explanation to support the answer.

None of the personal data collected is likely to be perceived as particularly private or intrusive: all data is provided by the employee through his/her contract with L'Oréal considering the first name/last name and professional email address of the employee is already available through L'Oréal intranet. Data is collected by a reuse of personal data from OA PASS for L'Oréal employees. For externals, L'Oréal collect personal data when the external arrives.

4.3 Describe how such personal data (sensitive, or considered particularly private) are necessary, and consider what would be the impacts for the data subjects, for L'Oréal or a third party if such data are not processed.

Not applicable.

4.4 Specify if the personal data processing involves children's data or relate to vulnerable categories of individuals (e.g. L'Oréal employees, children, influencers, volunteers).

The personal data processing relates to L'Oréal employees who are considered as "*vulnerable individuals*" considering the imbalance of powers between an employer and an employee.

Source and Reuse of personal data

4.5 Specify if the personal would be collected directly from the individuals, or if such personal data would be obtained from a third-party controller.

Personal data is collected by L'Oréal: for employees, personal data are obtained from OA PASS. For externals, L'Oréal collect personal data when the external arrives.

4.6 Specify if the personal data have already been processed in the past, in which case for what purpose(s) and how.

Personal data is collected by a reuse of personal data from OA PASS for L'Oréal employees. For externals, L'Oréal collect personal data when the external arrives.

4.7 Specify how long ago such personal data was collected, and if there are any changes in technology or context since then that would affect individuals' expectations.

Above mentioned personal data is mostly collected at the employee's arrival in the Group. No changes in technology or context occurred since then are likely to affect their legitimate expectations.

For employees, personal data have been already processed for internal administration management during the time the employee work for L'Oréal and after depending of the purpose.

4.8 Describe the new purposes for which the personal data are processed and assess if this new purpose is compatible with the previous purpose(s) or not (e.g. marketing versus research purposes).

Based on Article 29 Working Party's guidelines on purpose limitation (Opinion 03/2013), The new purpose pursued is compatible with the former purpose as:

- there is a link between such purposes: contact details are more or less implied in the initial purposes of collection;
- the context of initial collection by L'Oréal of employee's identity and contact detail is when they are joining the company and use of their data for HR processing activities;
- the personal data processed in the context of the new purpose are not sensitive;
- the use of the personal data for the new purposes is meant to have a positive impact on individuals;

Information of individuals

4.9 Describe how and when individuals would be informed.

L'Oréal employees are informed through the Global HR privacy policy by the mention below (extract of the Global HR privacy policy). This document must be updated, including in regard of the data retention period and legal basis. Privacy Policy for employee is provided to them upon their HR onboarding and remains available permanently directly on their HR account in their local language.

Management of IT devices at global level	Core data : · Professional identification Transactional data: · Professional allocations : serial number of tools, … · Journal of connections of workstations to the L'Oréal network	. Ensure consistency of IT policies at global level · Organize worldwide implementations of applications · Allow your Employer to inventory the devices (PC, screens, printers etc.) · Allow your Employer to inventory the softwares installed on workstations · Allow your Employer to organize remote control for assistance or maintenance purposes	· Legitime interest · Working contract (Employees) . Performance of an intra group contract where l'Oréal SA is a service provider	· Retention in process of evaluation.

For non-employees, data subjects should be informed directly by their employer, as L'Oréal contracts with providers must include a clause requiring provider to provide its employees with L'Oréal Privacy Policy. So L'Oréal privacy policies/notices included in agreements will have to be checked on a case-by-case basis and updated if required to include a similar information than provided for in the PP B2E.

4.10 Assess if GDPR requirements in terms of information would be met (Article 14 in case personal data would be obtained from a third-party controller, and Article 13 in case personal data would be obtained directly from the individuals).

The Privacy Policy for L'Oréal employees is provided to them upon their arrival and remains accessible at all times in their HR profile in their native language. Content of the Privacy Policy must be aligned with GDPR requirements as per article 13/14 and additional local privacy requirements if any.

For non-employees, data subjects should be informed directly by their employer, as L'Oréal contracts with providers must include a clause requiring provider to provide its employees with L'Oréal Privacy Policy. So L'Oréal privacy policies/notices included in agreements will have to be checked on a case-by-case basis and updated if required to include a similar information than provided for in the PP B2E.

4.11 Indicate if the information document (e.g. Privacy notice, Privacy Policy) would make a specific and clear reference about the legitimate interest pursued. In which case, refer and quote such paragraph.

For employees yes – Please refer to the extract of the Global Privacy Policy for employees reproduced in point 4.9 above.

For externals, by principle yes this should be included – However privacy notices/templates shared in contracts would have to be checked.

Personal data use and sharing

4.12 Describe if the personal data processing involves a new or innovative technology and highlight the impacts on the individuals.

The personal data processing does not involve any new or innovative technology.

4.13 Describe if this is a large-scale processing considering volume of personal data processed, number of individuals concerned as well as the geographical extent of the processing activity and its duration.

In accordance with recital 91 of GDPR and guidelines of the EDPB, the personal data processing is not a large-scale processing since this personal data processing is only relating to few categories of personal data and the retention period is limited.

4.14 Specify if the personal data will be shared with a third-party controller. In which case, provide detailed explanation who they are, why and how data sharing would take place.

The personal data will not be shared with any third-party controller.

Potential impacts on the individuals

4.15 Describe any potential impact of the personal data processing on individuals and individuals' interests/fundamental rights at stake.

In this processing, the personal data collected and processed from employees and externals who works both for L'Oréal, could have potential impact on individuals and individuals' interests.

The main impact for individuals, is the inability to work. Indeed, if L'Oréal doesn't process personal data to manage IT devices accesses, they couldn't have equipment to perform their tasks. Moreover, if no transactional data are processed the IT teams couldn't ensure the follow-up of activities. For example, if a computer falls and break down, the individual, thanks to personal data processed by L'Oréal IT teams, can communicate with them to have a new computer as soon as possible.

It is not a sensitive processing of personal data for individuals. The processing allows them to have access to a service provided by L'Oréal IT teams. There is no fundamental right impacted by this processing.

> *Examples: impacts can include physical, material, and moral damages: serious physical harm long-term harm (e.g. worsening of health due to improper care, or disregard of contraindication); long-term or permanent psychological harms; financial risk or financial loss as a result of a fraud or attempted phishing ; inability to work; exclusion from a benefit/a service or product/a contract; loss of evidence in the context of litigation; feeling of invasion of privacy with irreversible damage; feeling of vulnerability after a summons to court; feeling of violation of fundamental rights like discrimination, freedom of expression; victim of blackmailing ; lost opportunities like refusal of internships or employment; loss of employment; loss of customer data; missed career opportunity; employee monitoring; targeted*

online advertising on a private aspect that the individual wanted to keep confidential like pregnancy advertising or drug treatment; inaccurate or inappropriate profiling; receipt of unsolicited mail like spams; reuse of data published on websites for the purpose of targeted advertising (information to social networks, reuse for emailing) etc.

4.16 Assess for each potential impact their likelihood[3] and severity[4].

According to the 4.15 answer, the likelihood and the severity of the impact mentioned are limited.

Expectations of the individuals

4.17 Assess if the individuals would widely and reasonably expect their personal data to be used for the intended purposes (e.g. would they find it intrusive? be surprised?). Provide detailed explanations and if relevant, findings from a panel test to back up the answer.

It is a reasonable assumption that individuals wouldn't find this processing intrusive considering this is a very common and standard security measure implemented in any organisations for security reasons.

4.18 Describe which measures and how they would be implemented to ensure individuals keep control over use of their personal data.

Privacy Policies include contact details for individuals to exercise their rights in various ways (e.g. by email or postal means).

4.19 Describe what would be the impacts for L'Oréal if the individuals exercise their right to object or withdraw consent.

The impacts for L'Oréal would be important as it could lead to not provided to employees IT devices to allow them to perform their tasks efficiently. In this context, article 21 GDPR states that data controllers are able not to proceed with an object request should they have "compelling legitimate grounds", which would be the case in this instance.

Additional safeguards available

4.20 Is a privacy impact assessment (PIA) performed for project initiated? ~~YES~~ **NO**

If "YES" selected, please share the outcomes of the risk assessment, and specify which mitigation measures will be implemented

If "NO" selected, go to next question

There is no PIA (Privacy brief to be initiated).

4.21 Describe the additional controls/safeguards that would be adopted to minimize the impacts for the individuals, and how such additional controls/safeguards would be implemented.

Controls already in place:

- Data minimization is already implemented to collect personal data strictly necessary for the purposes above mentioned
- Access is restricted as only the relevant local IT support team has access to the support request and related personal data.

Additional controls to be implemented:

[3] Assess likelihood based on following levels: (i) negligible (impact would not materialize) ; (ii) limited (impact would be difficult to materialize) ; (iii) significant (impact would materialize) and (iv) maximum (impact would definitely materialize very easily)

[4] Assess severity based on following levels: (i) negligible (individuals would not be affected); (ii) limited (individuals would be affected and encounter minor difficulties); (iii) significant (individuals would encounter significant difficulties) and (iv) maximum (individuals would encounter significant and irreversible difficulties)

- Updating the global HR privacy policy to reflect the right information on the data processing (e.g. to withdraw mention of contract legal basis and to update the data retention)
- For non-employees: check contract templates to ensure they include a L'Oréal privacy notice/policy informing externals, and checking this mention is similar in content to the one provided in L'Oréal Global Privacy Policy B2E
- Investigate to ensure the process of informing externals is efficient and if not, determine alternative solutions to make it operational and effective (e.g. privacy notice automatically sent to externals upon their arrival)
- Perform a Privacy Brief

Examples: technical and organisational measures to ensure that the data cannot be used to take decisions or other actions with respect to individuals ("functional separation"),wide use of anonymisation techniques, aggregation of data, privacy-enhancing technologies, privacy by design, adding extra transparency, additional layers of encryption, multi-factor authentication, retention, restricted access, general and unconditional right to opt-out, other technical IT/SEC measures to protect data, reduce scope of the processing, data portability & related measures to empower data subjects, etc.)

STEP 5: OUTCOMES OF THE ASSESSMENT

~~The personal data processing can be based on legitimate interest as no alternative legal basis applies and the balancing test is favorable to the individuals.~~

~~The personal data processing must be based on an alternative legal basis.~~

The personal data processing can be based on legitimate interest with additional controls or safeguards.

Author(s): IT HDP and Group DPO Team

Date: 09/08/2022

Please keep a record of this LIA