**COMPANY\_NAME**

**GDPR ASSESSMENT REPORT**

***Confidential***

Dear Mr. …..

At your request, our law firm has carried out an audit of COMPANYNAME France with a view to evaluate its level of conformity with the General Data Protection Regulation (« ***GDPR*** »).

Considering the profile and activities of COMPANYNAME France, namely:

* a French subsidiary of an international group;
* legally and financially independent from its mother company;
* having mainly a B2B2B activity of integrator of products develops by other companies.

Considering also the fact that COMPANYNAME France:

* is very dependent of COMPANYNAME HQ for its business activities and HR activities;
* relies on third parties for various tasks such as security control, pay slips management and recruitment has no real marketing activity.

The audit had been focused mainly on the GDPR compliance of COMPANYNAME France in the context of its business activities (Part I), its HR activities (Part II) and for the internal access and external visitors control (Part III).

Mr. …… Ms. ….. and you were our main interlocutors for the performance of the audit. In addition, copies and extracts of business agreements entered into by COMPANYNAME France were provided by M. …..; there are attached thereto in exhibit.

The present report recapitulates in a table format the observations made during the audit. The assessment method is based on 3 levels of evaluation:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Adequate**: means that the GDPR obligation is fulfilled |  | **Insufficient** : means that the GDPR obligation is partly fulfilled or that the risk incurred by COMPANYNAME France is limited |  | Non adequate : means that the GDPR obligation is not fulfilled and the risk incurred by COMPANYNAME France is significant |

I remain at your disposal should you have any question about this report.

Yours sincerely,

|  |  |
| --- | --- |
|  |  |
|  |  |

**PART I – BUSINESS ACTIVITIES**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Object** | **Subject matter** | **GDPR** | **Assessment** | **Recommendation/measure** |
| **Business contacts of:**   * **existing customers** * **contractors** | **Personal data :**   * Name * Phone number * Email * Position | **Art. 4, 1**  For the purposes of this Regulation:  (1) ‘**Personal data’** means any information relating to an identified or identifiable natural person (‘data subject’); […]; | Adequate:   * Appropriate to the purpose of the processing | * Always ensure that the personal data processed is adequate, relevant and limited to what is necessary to the purpose of the processing. * As often as possible, avoid buying mailing lists. |
| **Consent** | **Consent exemption** | **Art. 6, 2**  Processing shall be lawful only if and to the extent that at least one of the following applies: […]  (2) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; […] | Insufficient:   * Copies and extracts of agreements provided show that all the agreements entered into by COMPANYNAME must be updated with GDPR provisions. | * If in the capacity of COMPANYNAME France, all the commercial agreements with existing customers must be updated to include GDPR provisions. * **A privacy policy** must be written and made available to existing customers and contractors by email. |
| **Processing** | **Personal data collection** | **Art. 4, 2**  (2) ‘**processing’** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; […] | Adequate:  Personal data obtained :   * by exchanging business cards * from people participating in local events where they leave business cards * by sales people networks (incl. LinkedIn) | * Always ensure that the personal data processed is adequate, relevant and limited to what is necessary to the purpose of the processing. * As often as possible, avoid buying mailing lists. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Object** | **Subject matter** | **RGPD** | **Assessment** | **Recommendation/measure** |
|  | * Direct collection | **Art. 13**  Information to be provided where personal data are collected from data subject. | Non adequate:   * Information required by GDPR art 13 is not provided. | **A privacy policy** containing the information required by art 13 and 14 of GDPR must be written and made available to existing customers and contractors by email.  *Can be individual email to each business contact or can be an emailing campaign.* |
| * Indirect collection | **Art. 14**  Information to be provided where personal data have not been obtained from data subject. | Non adequate:   * Information required by GDPR art 14 is not provided. |
|  | **Internal processing** | **Art. 4, 2)**  See above | Insufficient:   * No internal data processing policy * Internally personal data are processed erratically: some data are organised on a CRM database, some on excel files, some on the personal mobile phones of the employees, some on outlook databases | * Must be set up: * **An internal data processing policy;** * **A good practices policy**. * All the data must be centralised and kept in the CRM tool and then processed internally (organised, structured, extracted, updated, etc.) from the CRM Tool. * The CRM tool must be updated according to the publisher’s recommendations.   *If possible and not depending of HQ, a more efficient and EU CRM tool should be purchased.* |
|  | **Share and transfer of data** | **Art. 4, 2)**  See above | Insufficient:   * Data is shared between CompanyName France and CompanyName HQ (CompanyName HQ is not considered 3rd party, but part of the group) * Excel files with contacts are shared with CompanyName HQ once a year for Mobile World event in Barcelona. | **A privacy policy** informing the business contacts on how their data are shared between the companies of the group must be written and made available to them by email.  *Can be the same document as the one mentioned above.* |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Object** | **Subject matter** | **RGPD** | **Assessment** | **Recommendation/measure** |
|  | **Storage** | **Art. 4, 2)**  See above | Insufficient:  Data are stored in France but in various places inside the company: CRM database (extremely limited info), local file server, backup server and user laptop, email server, phone contacts list. | * Must be set up: * **A personal data storage policy** *(can be added to the data processing policy document)* **;** * **A good practices policy** (c*an be the same document as one mentioned above)* |
|  | **Profiling** | **Art. 4, 4)**  (4) ‘**profiling’** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements | No profiling performed |  |
|  | **Erasure / Destruction** | **Art. 4, 2)**  See above | Non adequate:   * No specific policy on personal data retention duration * No specific procedure for the erasure or destruction of personal data. | **A specific policy on personal data retention duration must be set up, together with specific erasure and destruction procedures.**  *(can be added to the data processing policy document)* |
| **Data subject Rights** | **Rectification** | **Art. 16** | Non adequate:   * No information is provided by COMPANYNAME France to the data subject as regard to its rights. | **A privacy policy** informing the business contacts on their rights must be written.  *(Can be the same document as the one mentioned above.)* |
| **Erasure / To be forgotten** | **Art. 17** |
| **Restriction of processing** | **Art. 18** |
| **Data Portability** | **Art. 20** |
| **To object** | **Art. 21** |
| **Security** | **Appropriate security**   * Confidentiality * Integrity * Reliability | **Art. 5, 1.** Personal data shall be: […]processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’)  **Art. 32**  Security of processing | Insufficient:   * No appropriate measure is in place to ensure the security of the personal data processed. However, because of the type of personal data, a breach of security will not have an impact on the privacy of the business contacts. | The setting up of the recommended measure should enable CompanyName France to fulfill this obligation. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Object** | **Subject matter** | **RGPD** | **Assessment** | **Recommendation/measure** |
|  | **Encryption** | **Art. 32**  Security of processing | Adequate:  No encryption is needed for the type of personal data processed. In addition, encrypting this data will compromise the quality of the relationships with the customers and contractors. |  |
| **Crisis management** | **Notification to CNIL**  **-** Privacy breach  - security incident | **Article 33** Notification of personal data breach to the CNIL (Supervisory Authority) **within 72 hours** after having become aware of it. | Non adequate:  Because CompanyName France has no internal policies on personal data protection, the company will be unable to know if a breach had occurred and to fulfill its obligation of notification within 72 hours. | The setting up of the recommended measure should enable CompanyName France to fulfill this obligation. |
| **Communication to the data subject**  **-** Privacy breach | **Article 34** Communication of a personal data breach to the data subject without undue delay. | Non adequate:  Because CompanyName France has no internal policies on personal data protection, the company will be unable to know if a breach had occurred and to fulfill its obligation under this article 34 of GDPR. | The setting up of the recommended measures should enable CompanyName France to fulfill this obligation. |

**PART II – HR ACTIVITIES**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Object** | **Subject matter** | **RGPD** | **Assessment** | **Recommendation/measure** |
| **Personal data of:**   * **Existing employees** * **Job applicants** | **Employees:**   * Name * Personal address * Date and place of birth * Social security number * Position * Salary * Taxes * Sick leaves data * Personal IP address | **Art. 4, 1**  For the purposes of this Regulation:  (1) ‘**Personal data’** means any information relating to an identified or identifiable natural person (‘data subject’); […]; | Adequate:   * Appropriate to the purpose of the processing   + HR management   + Social security   + Complementary health insurance | Always ensure that the personal data processed are adequate, relevant and limited to what is necessary to the purposes of the processing. |
|  | **Job applicants:**   * Name * Personal address * Age * Email * Phone number * Previous positions | Adequate:   * Appropriate to the purpose of the processing   + Recruitment management |
| **Consent** | **Consent exemption** | **Art. 6, 2**  Processing shall be lawful only if and to the extent that at least one of the following applies: […]  (2) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; […]  (3) processing is necessary for compliance with a legal obligation to which the controller is subject; | Adequate:   * Appropriate to the purpose of the processing |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Object** | **Subject matter** | **RGPD** | **Assessment** | **Recommendation/measure** |
| **Processing** | **Personal data collection** | **Art. 4, 2**  (2) ‘**processing’** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; […] | Adequate:   * Personal data obtained:   + on the CVs   + during the job interviews   + on the employment contracts   + on the sick leaves documents | Always ensure that the personal data processed are adequate, relevant and limited what is necessary to the purpose of the processing. |
| * Direct collection | **Art. 13**  Information to be provided where personal data are collected from data subject. | **Non adequate:**   * Information required by GDPR art 13 is not provided. | * **A specific agreement** must be signed between CompanyName France and CompanyName HQ * **An internal data processing policy** must be set up and implemented for HR data. * **A notice of information** should be sent to every prospective candidate invited to a job interview. |
| * Indirect collection | **Art. 14**  Information to be provided where personal data have not beed collected from data subject. | **Non adequate:**   * Information required by GDPR art 14 is not provided. |
|  | **Internal processing:** | **Art. 4, 2)**  See above | **Non adequate**:   * **HR data** is processed erratically in HQ and France on the HR Tool, File Server, Backup server, Email server, physical cabinets, HR rep laptop; * **HR Data** is stored on email server as per HR representative inbox. So, the IT department managing the email server may have access to data * There is no specific written agreement between CompanyName France and CompanyName HQ for the processing of French HR data; * There is no internal data processing policy specific to HR data. | * **A specific agreement** must be signed between CompanyName France and CompanyName HQ concerning HR data processed in HQ * **An internal data processing policy** must be set up and implemented for HR data.   (Can be the s*ame document as mentioned above*) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Object** | **Subject matter** | **RGPD** | **Assessment** | **Recommendation/measure** |
|  | **Share and transfer of data** | **Art. 4, 2)**  See above | **Non adequate**:  No specific data sharing and transfer procedures, although:   * HR Data is shared with CompanyName HQ * Salary, taxes and sick leaves data are share with UniverPay on a monthly bases * HR Data are also shared with Financial auditors and Insurance companies * Job applicants data are share with external consultants | * **A specific agreement** must be signed between CompanyName France and CompanyName HQ concerning HR data processed in HQ. * **An internal data processing policy** must be set up and implemented for HR data. * **An audit must be carried out with UniverPay** and **GDPR sub-contractor agreement should be signed** between CompanyName France and UniverPay. * **An audit must be carried out with external consultants** and **GDPR sub-contractors agreements should be signed** with each of them. * Confirmation of conformity to GDPR must be obtained from concerned financial auditors and insurance companies. |
|  | **Storage** | **Art. 4, 2)**  See above | **Non adequate**:   * HR Data is stored in HQ and in France in various places inside both companies: The HR Tool, File Server, Backup server, Email server, physical cabinets, HR rep laptop. | * **A specific agreement** must be signed between CompanyName France and CompanyName HQ concerning HR data storage in HQ (*can be the same document as the one mentioned above*) * **A storage policy** must be set up*(can be added to the data processing policy document specific to HR Data)* **;** |
|  | **Profiling** | **Art. 4, 4)**  (4) ‘**profiling’** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements | No profiling performed |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Object** | **Subject matter** | **RGPD** | **Assessment** | **Recommendation/measure** |
|  | **Erasure / Destruction** | **Art. 4, 2)**  See above | Non adequate:   * No specific policy on personal data retention duration * No specific procedure for the erasure or destruction of HR data. | **A specific policy on HR data** retention duration must be set up, together with **specific erasure and destruction procedures**. |
| **Rights** | **Rectification** | **Art. 16** | Non adequate:   * No information is provided by COMPANYNAME France to the employees and prospective candidates on their rights. | * **An internal data processing policy** must be set up and implemented for HR data. * **Employment contract of each employee should be updated by an amendment.** |
| **Erasure / To be forgotten** | **Art. 17** |
| **Restriction of processing** | **Art. 18** |
| **Data portability** | **Art. 20** |
| **To object** | **Art. 21** |
| **Security** | **Guaranty of security**   * Confidentiality * Integrity * Reliability | **Art. 5, 1.** Personal data shall be: […]processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’)  **Art. 32**  Security of processing | Non adequate:   * No real precaution is taken to guaranty the security of the HR data processed; * No information provided on the level of security assured by CompanyName HQ on the French HR data; * IT department managing the email server of HR representative may have access to HR data. | The setting up of the recommendations mentioned previously should enable CompanyName France to fulfill this obligation. |
|  | **Encryption** | **Art. 32**  Security of processing | Non adequate:   * No information provided on the level of encryption assured by CompanyName HQ on the French HR data; * No encryption is performed on the data stored on the HR rep laptop or data server. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Object** | **Subject matter** | **RGPD** | **Assessment** | **Recommendation/measure** |
| **Crisis management** | **Notification to CNIL**  **-** Privacy breach  - security incident | **Article 33** Notification of personal data breach to the CNIL (Supervisory Authority) **within 72 hours** after having become aware of it. | Non adequate:   * Because CompanyName France has no internal policies on HR data protection, the company will be unable to know if a breach had occurred and to fulfill its obligation of notification within 72 hours. | The setting up of the recommendations mentioned previously should enable CompanyName France to be prepared and to fulfill this obligation. |
| **Communication to the data subject**  **-** Privacy breach | **Article 34** Communication of a personal data breach to the data subject without undue delay. | Non adequate:   * Because CompanyName France has no internal policies on HR data protection, the company will be unable to know if a breach had occurred and to fulfill its obligation under this article 34 of GDPR. |

**PART III – PREMISES ACCESS AND EXTERNAL VISITORS CONTROL**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Object** | **Subject matter** | **RGPD** | **Assessment** | **Recommendation/measure** |
| **Personal data of:**   * **Employees** * **External visitors** | **Employees:**   * Name * Premises access log (date, time and duration of access) | **Art. 4, 1**  For the purposes of this Regulation:  (1) ‘**Personal data’** means any information relating to an identified or identifiable natural person (‘data subject’); […] | Adequate:   * Appropriate to the purpose of the processing | Always ensure that the personal data processed are adequate, relevant and limited what is necessary to the purpose of the processing. |
|  | **External visitors:**   * Name * ID card * Images | **Art. 5, 1**  Personal data shall be:  (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’) | Insufficient:   * Unable to determine if the images processed by the video surveillance system are relevant and limited to what is necessary to the purposes of the processing | An audit should be carried out with the company in charge of the video surveillance and a GDPR sub-contractor agreement should be signed with this company. |
| **Consent** | **Consent requirements** | **Art. 6, 1**  Processing shall be lawful only if and to the extent that at least one of the following applies: (1) the data subject has given consent to the processing of his or her personal data for one or more specific purposes  **Art. 7**  Conditions of consent | Insufficient:   * Employees’ access: the provision specified in the employment contracts is no longer valid. * External visitors: No notice is given of the video surveillance control. | * **Employment contract of each employee should be updated by an amendment.** * **An audit should be carried out with the company in charge of the video surveillance** and **a GDPR sub-contractor agreement** should be signed with this company. * **A notice must be made visible** to the external visitors before the checkpoint. |
| **Processing** | **Personal data collection** | **Art. 4, 2)**  (2) ‘**processing’** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; […] | Adequate:   * Personal data obtained:   + from the CVs   + during the job interviews   + from the employment contracts   + from the sick leaves documents | Always ensure that the personal data processed are adequate, relevant and limited what is necessary to the purpose of the processing. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Object** | **Subject matter** | **RGPD** | **Assessment** | **Recommendation/measure** |
|  | * Direct collection | **Art. 13**  Information to be provided where personal data are collected from data subject. | Non adequate:   * Information required by GDPR art 13 is not provided. | * **Consent document must be signed** by each employee of CompanyName France * **An audit should be carried out with the company in charge of the video surveillance** and **a GDPR sub-contractor agreement** should be signed with this company. * **A notice must be made visible** to the external visitors before the checkpoint. |
| * Indirect collection | **Art. 14**  Information to be provided where personal data have not been collected from data subject. | No indirect collection |  |
|  | **Internal processing:** | **Art. 4, 2)**  See above | **Non adequate**:   * No information provided on how the personal data of employees’ access and external visitors is processed. | **An internal data processing policy** must be set up and implemented. |
|  | **Share and transfer of data** | **Art. 4, 2)**  See above | **Adequate**:   * Videos are shared with by the security company to the police only | Ensure on a regular basis that the procedure has not change. |
|  | **Storage** | **Art. 4, 2)**  See above | **Non adequate**:   * No information provided on how the personal data of employees’ access and external visitors is stored. | * **An internal data processing policy** must be set up and implemented. * **An audit should be carried out with the company in charge of the video surveillance** and **a GDPR sub-contractor agreement** should be signed with this company. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Object** | **Subject matter** | **RGPD** | **Assessment** | **Recommendation/measure** |
|  | **Profiling** | **Art. 4, 4)**  (4) ‘**profiling’** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements | No profiling performed |  |
|  | **Erasure / Destruction** | **Art. 4, 2)**  See above | Non adequate:   * No information provided on how long the personal data of employees’ access and external visitors is kept and how it is destroyed. | * **An internal data processing policy** must be set up and implemented. * **An audit should be carried out with the company in charge of the video surveillance** and **a GDPR sub-contractor agreement** should be signed with this company. |
| **Rights** | **Rectification** | **Art. 16** | Non adequate:   * No information is provided by COMPANYNAME France to the employees and external visitors on their rights. |
| **Erasure / to be forgotten** | **Art. 17** |
| **Restriction of processing** | **Art. 18** |
| **Data Portability** | **Art. 20** |
| **To object** | **Art. 21** |
| **Security** | **Guaranty of security**   * Confidentiality * Integrity * Reliability | **Art. 5, 1.** Personal data shall be: […]processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’)  **Art. 32**  Security of processing | Non adequate:   * No information provided on the level of security assured by CompanyName France and the surveillance company on this data. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Object** | **Subject matter** | **RGPD** | **Assessment** | **Recommendation/measure** |
|  | **Encryption** | **Art. 32**  Security of processing | Non adequate:   * No information provided on the level of encryption assured by CompanyName France and the surveillance company on this data. | * **An internal data processing policy** must be set up and implemented. * **An audit should be carried out with the company in charge of the video surveillance** and **a GDPR sub-contractor agreement** should be signed with this company. |
| **Crisis management** | **Notification to CNIL**  **-** Privacy breach  - security incident | **Article 33** Notification of personal data breach to the CNIL (Supervisory Authority) **within 72 hours** after having become aware of it. | Non adequate:   * Because CompanyName France has no internal policies on HR data protection, the company will be unable to know if a breach had occurred and to fulfill its obligation of notification within 72 hours. | The setting up of the recommendations mentioned previously should enable CompanyName France to be prepared and to fulfill this obligation. |
| **Communication to the data subject**  **-** Privacy breach | **Article 34** Communication of a personal data breach to the data subject without undue delay. | Non adequate:   * Because CompanyName France has no internal policies on HR data protection, the company will be unable to know if a breach had occurred and to fulfill its obligation under this article 34 of GDPR. |