

**[NAME OF THE LUXEMBOURGISH COMPANY]**

**[COMPANY TYPE, E.G. SOCIÉTÉ ANONYME / SOCIÉTÉ À RESPONSABILITÉ LIMITÉE]**

**SHARE CAPITAL: [optional]**

**REGISTERED OFFICE: [●], L- [\*\*\*\*] LUXEMBOURG**

**R.C.S. LUXEMBOURG: [●]**

**(THE "COMPANY")**

---

## **GDPR COMPLIANCE ASSESSMENT FORM**

**PLEASE COMPLETE & RETURN VIA MAIL OR EMAIL**

---

Reference number of the Company's file @ Kaufhold & Reveillaud, if applicable:

**REFKR** \_\_\_\_\_

This "tick-the-box" form allows Kaufhold & Reveillaud to assess your GDPR compliance burden and develop an effective proposal. In short, it amounts to a GDPR compliance roadmap.

**Please tick the appropriate boxes:**

Name of the Company:

What company within the Company's group will be the Data Controller?

The Company itself  or another Luxembourg company of the same group

Name of company: \_\_\_\_\_

Will the company act as Data Controller and/or GDPR compliance manager for other affiliates of the same group? If yes, please name and list them:

---

Does the Company have:

An in-house server solution and/or a  cloud-computing solution?

In what jurisdiction are the respective servers based? \_\_\_\_\_

Does the Company conduct commercial activity? Yes  No

If yes, please describe: \_\_\_\_\_

Is the Company regulated/licensed? Yes  No

If yes, what type of activity and kind of license (e.g. PSF / Banking)?

\_\_\_\_\_

Is there already a Data Protection Officer (DPO) somewhere within the group?

Yes  No

Details about the individual in the group who will be appointed DPO or Data Protection Person of Contact (DPPoC):

Name of [DPO / DPPoC]: \_\_\_\_\_

Email address of [DPO / DPPoC]: \_\_\_\_\_

Employees: Yes  No  / if yes, how many: \_\_\_\_\_

Are there any Executives (managers/directors) of the Company under an employment agreement? Yes  No

If yes, please list them by name: \_\_\_\_\_

Are the Ultimate Beneficial Owners of the Company identified?: Yes  No

Who are the shareholders of the Company?

Legal Entities  and/or Natural Persons

Does the Company have (a) website(s)? Yes  No

If yes, please list below the domains:

\_\_\_\_\_

Does the Company have contractors? Yes  No

Legal Counsel: \_\_\_\_\_

Accountancy: \_\_\_\_\_

Domiciliation and Corporate Services Provider: \_\_\_\_\_

IT/Computing Service Provider: \_\_\_\_\_

Tax advice: \_\_\_\_\_

Other(s): \_\_\_\_\_

## **Obligation to maintain “Records of Processing Activities” according to the terms of Article 30 of GDPR:**

**The Company employs 250 or more persons**

No  Yes  In the near future

**The Company routinely processes Personal Data**

No  Yes  In the near future

**The Company’s processing is likely to result in a risk to the rights and freedoms of data subjects (= natural persons)**

No  Yes  Maybe  Description of such risk \_\_\_\_\_

**The Company processes personal data relating to:**

None of the below items in this section are applicable

- Race
- Ethnicity
- Political opinions
- Religious believes
- Health
- Sex life and/or sexual orientation
- Philosophical beliefs
- Trade union membership
- Genetic data and/or biometric data for the purpose of uniquely identifying a natural person
- Personal data relating to criminal convictions and offenses

### **International transfers of personal data out of the European Economic Area (EEA)**

If personal data is processed in jurisdictions other than the ones listed below in this section, please list them by name here:

\_\_\_\_\_

If the personal data is processed in one of the following jurisdictions, no specific legal advice must be sought at the current date:

EU27: Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden.

- United Kingdom (Please tick the box if data is processed in this jurisdiction)

Iceland, Liechtenstein and Norway (= members of EEA without EU28)

Adequacy Decisions: Andorra, Argentina, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay.

- Canada (only for commercial organizations subject to the Canadian “Personal Information Protection and Electronic Documentation Act”); please tick the box if data is processed in this jurisdiction
- Japan (only for business operators handling personal information and subject to the Japanese “Act on the Protection of Personal Information” as outlined by the “Supplementary Rules set”)
- United States of America (limited to the EU-US Privacy Shield framework); please tick the box if data is processed in this jurisdiction

### **Obligation to appoint a Data Protection Officer and/or a carry out a Data Protection Impact Assessment**

**The Company’s processing is “likely to result in a high risk to the rights and freedoms of natural persons”**

No  Yes

**If YES**, the processing is done via or will result in

- Evaluation or scoring, including profiling and predicting (e.g. creditworthiness)
- Tasking decisions and/or automated decision-making with legal or similar significant effect (e.g. leading to discrimination)

- Taking decisions on data subjects that produce “legal effects concerning the natural person” or which “similarly significantly affects the natural person” (e.g. the processing may lead to the exclusion or discrimination against individuals)
  - Systematic monitoring: processing used to observe, monitor or control data subjects, including data collected through “systematic monitoring of a publicly accessible area”
  - Sensitive data
  - Data processed on a large scale, taking into consideration: number, volume, duration, geographical extent
  - Datasets with different purposes that have been matched and/or combined
  - Data concerning vulnerable data subjects
  - Innovative use or applying technological or organizational solutions, (e.g. access based on fingerprint and facial recognition)
  - Cross-border data transfers outside the European Union
  - Processing “prevents data subjects from exercising a right or using a service or a contract”
  - Processing operations that consist of or include regular and systematic control of the activities of the employees – if they could have legal effects for employees or affect them in a significant way
  - File processing operations likely to contain personal data of the entire national population, if such a DPIA has not already been carried out as part of a general impact assessment.
  - Processing operations for scientific or historical research or for statistical purposes
  - Processing operations that consist of systematic tracking of the location of natural persons
  - Other: Description of processing and related risk
-