

CHECKLIST FOR A CONTROLLER AND PROCESSOR AGREEMENT UNDER GDPR

Nicola Benz | Ronald Kogens

1. The agreement must include the following details:

- ☐ the subject matter and duration of the processing;
- ☐ the nature and purpose of the processing;
- ☐ the type of personal data and categories of data subject; and
- ☐ the obligations and rights of the controller, such as
 - o right to determine the purpose and means of processing,
 - o right to instruct the processor, and obligation on the processor to comply with instructions of the controller,
 - o right to conduct audits and inspections of the processor.

The rights and obligations can be found in more detail below.

2. The agreement should include the following compulsory terms:

- ☐ the processor must only act on the written instructions of the controller (unless required by law to act without such instructions);
- ☐ the processor must ensure that people processing the data are subject to a duty of confidence;
- ☐ the processor must take appropriate measures to ensure the security of processing;
- ☐ the processor may only engage a sub-processor with the prior written consent of the controller. Where a general consent to sub-processors is given, the processor is obliged only to inform the controller of individual planned changes to its sub-processors in advance and to give the controller the possibility to object;
- ☐ the processor must assist the data controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;

- ☐ the processor must assist the data controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- ☐ the processor must delete or return all personal data to the controller as requested at the end of the agreement; and
- ☐ the processor must submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 GDPR obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

3. As a matter of good practice, the agreements should:

- ☐ state that nothing within the contract relieves the processor of its own direct responsibilities and liabilities under the GDPR; and
- ☐ reflect any indemnity that has been agreed.

Processors' responsibilities and liabilities checklist

1. In addition to the Article 28 (3) GDPR contractual obligations set out in the controller and processor agreements checklist above, a processor has the following direct responsibilities under the GDPR. The processor must:

- ☐ only act on the written instructions of the controller (Article 29 GDPR);
- ☐ not use a sub-processor without the prior written authorisation of the controller (Article 28 (2) GDPR);
- ☐ co-operate with supervisory authorities in accordance with Article 31 GDPR;
- ☐ ensure the security of its processing in accordance with Article 32 GDPR;
- ☐ keep records of its processing activities in accordance with Article 30 (2) GDPR;
- ☐ notify any personal data breaches to the controller in accordance with Article 33 GDPR;
- ☐ employ a data protection officer if required in accordance with Article 37 GDPR; and
- ☐ appoint (in writing) a representative within the European Union if required in accordance with Article 27 GDPR.

2. A processor should also be aware that:

- ☐ it may be subject to investigative and corrective powers of supervisory authorities under Article 58 GDPR;
- ☐ if it fails to meet its GDPR obligations
 - o it may be subject to an administrative fine under Article 83 GDPR;
 - o it may be subject to a penalty under Article 84 GDPR; and
 - o it may have to pay compensation under Article 82 GDPR.

Checklist based on a document made public by the UK Information Commissioner's Office: GDPR / Accountability and governance / Contracts and Art. 28 (3) GDPR

WHO IS FRORIEP?

Founded in Zurich in 1966, Froriep is one of the leading law firms in Switzerland, with offices in Zurich, Geneva and Zug, as well as foreign offices in both London and Madrid, serving clients seeking Swiss law advice.

We have grown a domestic and international client base ranging from large international corporations to private clients. Our unique, truly integrated, international structure mirrors our strong cross-border focus. We value and promote continuity and strong client relationships. Our teams are tailor-made, assembled from every practice area and across our network of offices.

Many of our lawyers are recognised as leaders in their practice areas, and our clients benefit from our in-depth knowledge and the rich diversity of talents, languages and cultures that makes our lawyers particularly versatile and adaptive.

ZURICH

Bellerivestrasse 201
CH-8034 Zurich
Tel. +41 44 386 60 00
Fax +41 44 383 60 50
zurich@froriep.ch

GENEVA

4 Rue Charles-Bonnet
CH-1211 Geneva 12
Tel. +41 22 839 63 00
Fax +41 22 347 71 59
geneva@froriep.ch

ZUG

Grafenaustrasse 5
CH-6302 Zug
Tel. +41 41 710 60 00
Fax +41 41 710 60 01
zug@froriep.ch

LONDON

17 Godliman Street
GB-London EC4V 5BD
Tel. +44 20 7236 6000
Fax +44 20 7248 0209
london@froriep.ch

MADRID

Antonio Maura 10
ES-28014 Madrid
Tel. +34 91 523 77 90
Fax +34 91 531 36 62
madrid@froriep.ch

© Froriep Legal AG 2018. This Newsletter contains general information on legal developments in Switzerland and does not provide advice in specific matters. The reproduction is authorised, provided the source is acknowledged.