SKANSKA

Skanska´s GDPR requirements and contract terms for subcontracting

03.07.2023

Skanska´s GDPR requirements and contract terms for subcontracting

Content

1. Background and objective 3
2. Definitions 3
3. Requirements 4
4. Transfer of personal data 4
5. IT-security 4
6. Audit 5
7. Engaging sub-processors 5
8. Damages and compensation 6
9. Order of validity of contract documents 6
10. Term 6
11. Governing law and dispute resolution 6

1. Background and objective

These requirements and terms contain Skanska´s GDPR requirements and terms for subcontracting when a subcontractor gains access and processes personal data as a Processor for which Skanska is the data Controller in accordance with the applicable data protection legislation (“Data Protection Legislation”).

The objective of these terms and requirements is to form a frame for Data Processing Agreement (“DPA”) to comply with the requirements in the Data Protection Legislation for a written agreement between Controller and Processor.

2. Definitions

The terms used in the DPA shall have the same meaning as assigned to them below and in the Data Protection Legislation, which inter alia imply that:

(a) The term **personal data** means any information that, directly or indirectly, can identify a living natural person.

(b) The term **processing** means any operation or set of operations performed regarding personal data, whether or not performed by automated means, for example collection, recording, organization, storage, adaptation or alteration, retrieval, gathering, use, disclosure by transmission, dissemination or otherwise making information available, alignment or combination, blocking, erasure or destruction.

(c) The term **data controller** means anyone who alone or jointly with others determines the purposes and means of the processing of personal data.

(d) The term **data processor** means a anyone who processes personal data on behalf of the data controller.

(e) The term **sub-processor** means a sub-contractor that is engaged by Processor. The sub-processor processes personal data on behalf of Controller in accordance with the sub-processor’s obligation to provide its services to Processor.

(f) The term **standard data protection clauses** adopted by the EU-Commission means standard contractual clauses regulating the transfer of personal data to third countries and that have been adopted by the EU Commission in accordance with Commission Decision C(2010)593 of 5 February 2010 or corresponding decision replacing such decision; and

(g) The term **Data Protection Legislation** means applicable data protection legislation. As from 25 May 2018, Regulation (EU) 2016/679 of the European Parliament of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation; the “GDPR”) and such national legislation implementing the GDPR is the applicable data protection legislation.

3. Requirements

Processor undertakes to process the personal data that it has access to under the Agreement on behalf of Controller, for the purpose of fulfilling the Agreement and during the agreement term. Processor further undertakes:

(a) To process the personal data in accordance with the Data Protection Legislation, the Agreement, the Data Processing Agreement, and any other documented instructions from Controller. Processor may, however, without instructions process information required by laws of the European Union or national legislation in a member state to which Processor is subject, but shall inform Controller of such requirement prior to processing, provided that Processor is not prohibited to give such information with reference to important grounds of public interest.

(b) Not to use or utilize personal data transferred to or transferred by Processor, collected to or collected by Processor, produced to or produced by Processor or any other way processed personal data under the DPA in its business.

(c) To keep the personal data confidential and not to disclose the personal data to any third parties or in any other way use the personal data in contradiction with the Agreement and the DPA. Processor shall also ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) To assist Controller, considering the nature of the processing, by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Controller's obligation to respond to and to fulfil requests from data subjects exercising their rights laid down in Chapter III of the GDPR; and

(e) To assist Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR (implement security measures, manage personal data breaches, conduct data privacy impact assessments and participate in prior consultations with the supervisory authority) taking into account the nature of the processing and the information available to Processor.

4. Transfer of personal data

Processor may not transfer person data to a third country or to an international organization outside EU/EEA (together “Third countries”) unless Controller has specifically requested or approved to do so. Such written approval should be requested and provided in writing to every entity and/or transmission receiver separately.

5. IT-security

Processor implements all appropriate technical and organisational measures necessary in order to ensure a level of security, as required pursuant to the Data Protection Legislation (Article 32 of the GDPR (32 § Data Protection Act (523/1999)) and other measures necessary in order for Processor to comply with the security requirements set out in the Agreement or that are otherwise required by Controller with reference to the DPA)

Processor undertakes to inform Controller of the technical and organisational measures, which it will implement in order to protect the personal data processed on behalf of Controller. In this context, see security instructions described in Appendix 1. If Processor makes changes that could affect the protection of personal data, Controller shall be informed of this well in advance before such changes are implemented.

In the event of data breach or any potential violation of information security, Processor shall notify Controller without delay after becoming aware of the infringement of information security of personal data or any other violation of Data Protection Legislation, this DPA or the instructions of Controller. As a part of the notification, Processor must inform Controller without delay and in writing all the necessary information about the disturbance and the related measures, especially:

(a) a description of the nature of the infringement of information security, including the information of registered groups and estimated number of registered persons affected by the infringement along with the information required by Data Protection Legislation

(b) necessary information regarding to the statutory obligations and fulfillment of the contractual obligations of Controller. These obligations shall be based, inter alia, Data Protection Legislation, agreements made with third parties and/or a request, a guidance and/or a ruling made by the supervisory authority or a tribunal.

(c) necessary information for preventing similar infringements of the information security and information required for the notifications made for the registered persons and possible third parties.o

6. Audit

Processor shall grant Controller access to all information required in order to verify that the obligations set out in the DPA are complied with. Processor shall facilitate and participate in audits, including inspections, carried out by Controller or a governmental authority or by a third party authorized by Controller. If Controller uses a third party to carry out the audit, that third party shall not be a competitor of Processor and shall undertake confidentiality in relation to Processor's information.

Processor shall immediately inform and consult with Controller in the event that a supervisory authority initiates or takes any action in relation to Processor with regard to the processing of personal data under the Agreement or the DPA.

7. Engaging sub-processors

Processor may not engage or replace a sub-processor for the performance of Processor's processing of personal data under the DPA, without obtaining a written approval from Controller in advance.

8. Damages and compensation

Processor shall, without limitation, hold harmless and indemnify Controller in the event of damage that is attributable to Processor's processing of personal data in breach of the DPA or the Data Protection Legislation. For the avoidance of doubt, administrative fines are imposed on the Party in breach of its obligations and, in consequence, neither Party will bear the other Party's administrative fines.

Processor's compensation under the Agreement includes compensation for Processor's undertakings under the DPA unless otherwise stated in writing by Parties.

9. Order of validity of contract documents

This DPA is irremovable part of the Agreement. If the terms of the Agreement and terms of this DPA are divergent or otherwise in contradiction, this DPA shall prevail.

10. Term

The DPA is effective from its signing and for as long as Processor processes personal data on Controller's behalf.

In the event that Processor is in breach of its obligations under the DPA or Data Protection Legislation and fails to remedy the deficiency within thirty (30) days of Processor being notified of the breach, or within the time period agreed between the Parties, Controller has the right to terminate the Agreement with immediate effect or the longer period of notice notified by Controller.

When the Agreement expires or terminates, Processor shall, based on Controller's instructions, delete or return to Controller without any additional cost, in a manner acceptable to Controller, all personal data, and delete existing copies unless storage of personal data is required pursuant to European Union law or the Member State's national law. Processor undertakes to actively seek instructions from Controller without delay.

11. Governing law and dispute resolution

The DPA shall be governed by and construed in accordance with Finnish law, with the exception of conflict of law rules.

Disputes regarding interpretation and application of the DPA shall be settled in accordance with the provisions in the Agreement regarding dispute resolution.

In the absence of provisions regarding dispute resolution in the Agreement, this section shall apply: Disputes arising in connection with the DPA shall be finally settled in arbitration in accordance with the Finnish Arbitration Act (967/1992, as amended).

The arbitration shall be held in Helsinki by one arbitrator and the arbitral proceedings shall be conducted in the English language, but submissions and evidence may be provided, and witnesses heard either in Finnish, Swedish or English. Confidentiality shall apply to the arbitration and the arbitration ruling.