

Joint Controller Arrangement between

Coloplast A/S, Denmark, Humlebaek ('HQ')

and

local Coloplast Group Entity ('Group Entity')
(see Appendix 1)

Where two or more controllers **jointly determine** the purposes and means of processing, they shall determine their respective responsibilities for **compliance** with the obligations under the GDPR in a **transparent** manner, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an **arrangement** between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The **arrangement** may designate a contact point for data subjects.
(Art. 26 GDPR)

§ 1

(1) This arrangement outlines the rights and obligations of the controllers (hereinafter also referred to as "Parties") for the joint processing of personal data. The Group Entity of Coloplast and Coloplast A/S (HQ) have joint controllership specifically regarding the obtaining of consents, whether online or offline, for the purposes of processing information about data subjects, including health data, in various respects to support the Coloplast business model. The arrangement applies to the obtaining of consents from data subjects for data processing which allow both Parties to process personal data, including consents for marketing. The data subjects in question may be a) consumers (end-users), b) customers (e.g. HCP's), c) patients and/or d) clinical trial and research subjects. The Parties have jointly determined the purposes and means of processing personal data in accordance with Article 26 GDPR.

(2) Both Parties have access to such information about the data subjects and may process data within the scope of the purpose or purposes for which the data has been collected. Data is processed first and foremost in SalesForce CRM-system. The Parties determine the sections in which personal data are processed under joint controllership (Article 26 GDPR).

(3) For the other sections of processing, where the Parties do not jointly determine the purposes and means of data processing, each Party is either a controller pursuant to Article 4(7) GDPR or a data processor pursuant to Article 4(8) GDPR for the other Party. As far as the Parties are joint controllers pursuant to Article 26 GDPR, it is arranged as follows:

§ 2

(1) The main responsibility for obtaining consent correctly (i.e. for consent validity) lies with the obtaining Group Entity in collaboration with HQ, whereas HQ and the Group Entity share responsibility for keeping data updated. HQ will eventually delete or anonymize data when it is no longer necessary or otherwise needed.

(2) HQ shall receive and reply to any data subject requests and exercise of rights and shall handle all data breach notifications (via CPBC).

§ 3

Each Party shall ensure compliance with the legal provisions of the GDPR, particularly in regard to the lawfulness of data processing under joint controllership. The Parties shall take all necessary technical and organisational measures to ensure that the rights of data subjects, in particular those pursuant to Articles 12 to 22 GDPR, are guaranteed at all times within the statutory time limits.

§ 4

(1) The Parties shall store personal data in a structured, commonly used, and machine-readable format.

(2) Group Entity shall ensure that only personal data which are strictly necessary for the legitimate conduct of the process are collected and/or for which the purposes and means of processing are specified by Union or national law. Moreover, both Parties agree to observe the principle of data minimisation within the meaning of Article 5(1)(c) GDPR.

§ 5

The Parties commit themselves to provide the data subject with any information referred to in Articles 13 and 14 of the GDPR in a concise, transparent, intelligible, and easily accessible form, using clear and plain language. The Parties agree that the Group Entity shall provide the information referred to in Article 13 where personal data (consent) are collected from the data subject locally, whereas HQ shall provide the information referred to in Article 14 in other situations where personal data have not been obtained from the data subject.

§ 6

The data subject may exercise his or her rights under Articles 15 to 22 GDPR against each of the joint controllers, cf. Article 26(3) GDPR. Subject requests shall be referred to CPBC without undue delay.

§ 7

(1) HQ shall receive and reply to any data subject requests and exercise of rights (via CPBC) and shall handle all data breach notifications. For further information, see [Data breaches and subject requests \(coloplast.com\)](#).

(2) If necessary, the Parties shall provide each other with the necessary information from their respective operating range. Competent contact persons for the Parties are Senior Privacy

Counsel, Claus Møller Thamdrup (Coloplast A/S) and the contact person identified in **Appendix 1** for each Group Entity. Each Party must inform the other Party immediately of any change of contact person.

§ 8

(1) If a data subject exercises his or her rights against one of the Parties, in particular of the rights of access, correction, or deletion of his or her personal data, the Parties are obliged to forward this request to the other Party without undue delay. This applies irrespective of the general obligation to guarantee the right of data subjects. The Party receiving the request must immediately provide the information within its operating range to the requesting Party.

(2) If personal data are to be deleted, the Parties shall inform each other in advance. A Party may object to the deletion for a legitimate interest, for example, if there is a legal obligation to retain the data set for deletion.

§ 9

The Parties shall inform each other immediately if they notice errors or infringements regarding data protection provisions during the examination of the processing activities.

§ 10

The Parties undertake to communicate the essential content of the joint controllership arrangement to the data subjects upon request, cf. Article 26(2) GDPR.

§ 11

HQ is the primary responsible to inform the relevant supervisory authority and the data subjects affected by a violation of the protection of personal data in accordance with Articles 33 and 34 GDPR. The Parties shall inform each other about any such notification to the supervisory authority without undue delay. The Parties also agree to forward the information required for the notification to one another without undue delay.

§ 12

If a data protection impact assessment pursuant to Article 35 GDPR is required, the Parties shall support each other to provide the DPIA in a timely manner.

§ 13

Documentations within the meaning of Article 5(2) GDPR, which serve as proof of proper data processing, shall be archived by each Party beyond the end of the arrangement in accordance with legal provisions and obligations.

§ 14

(1) Within their operating range, the Parties shall ensure that all employees authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality in accordance with Article 32(4) GDPR for the duration of their employment, as well as after termination of their employment. The Parties shall also ensure that they observe the data secrecy provisions prior to taking up their duties and are familiarised with the data protection legislation and rules relevant to them.

(2) The Parties shall independently ensure that they are able to comply with all existing storage obligations with regard to the data. For this purpose, they must implement appropriate technical and organisational measures, cf. Article 32 *et seq.* GDPR. This applies particularly in the case of termination of the arrangement.

(3) The implementation, default-setting, and operation of the systems shall be carried out in compliance with the requirements of the GDPR and other regulations. In particular, compliance with the principles of data protection by design and data protection by default will be achieved through the implementation of appropriate technological and organisational measures corresponding to the state of the art.

(4) The Parties agree to store personal data digitally on protected servers.

§ 15

(1) The Parties commit themselves to conclude a contract in accordance with Article 28 GDPR when engaging processors within the scope of this arrangement and to obtain the written consent of the other Party before concluding the contract.

(2) The Parties shall inform each other in a timely manner of any intended change with regard to the involvement or replacement of subcontracted processors. The Parties shall only commission subcontractors who meet the requirements of data protection legislation and the provisions of this arrangement. The Parties are obligated to make appropriate contractual arrangements in accordance with the law and to take controlling measures to guarantee the protection and security of personal data, even in the case of additional third-party services.

§ 16

The Parties shall include the processing operations in the records of processing activities pursuant to Article 30 (1) GDPR, in particular with a comment on the nature of the processing operation as one of joint or sole responsibility.

§ 17

Notwithstanding the provisions of this arrangement, the Parties shall be liable for damages resulting from processing that fails to comply with the GDPR. In external relations, the Parties are jointly liable to the data subjects concerned.

§ 18

(1) This document codifies what has been the *de facto* arrangement between the Parties since 25 May 2018.

(2) This arrangement outlines the respective responsibilities of the Parties for joint data controllership without signing.

Effective as of August 2021

APPENDIX 1

See: *Excel sheet: Contact Persons*

SAMPLE