

1. Purpose

The purpose of this Global Policy is to assist Convatec employees with identifying the correct lawful basis and requirements for processing personal data which they undertake or plan to undertake, and the obligations which go with that lawful basis.

2. Scope

This Policy applies to all employees globally, independent contractors, or Third Party Intermediaries who are involved in the processing of personal data for or on behalf of Convatec. This document covers all Convatec subsidiaries, business units and Franchises.

3. Policy

This policy outlines how personal data must be assessed and managed in accordance with local data protection laws, any personal data processed by (or on behalf of) Convatec must be lawful, fair, and transparent. Personal Data may only be processed after a lawful basis has been identified, approved, and documented.

Lawful basis is determined by the purpose of the collection and relationship with the data subject. There are six (6) available lawful basis criteria for personal data processing which are set out and explained in this document. At least one of the six lawful basis criteria must apply whenever personal data is being processed by or on behalf of Convatec. Personal data should only be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. If you can reasonably achieve the same purpose without the processing of personal data, the lawful basis will be invalid.

4. Privacy Accountability Framework Integration

This policy underpins the [Privacy Accountability framework](#) (PAF) and supports the requirement under **Appendix F** of that policy to put in place “records of processing and Lawful basis”. This policy shall ensure that:

- a) there is a clear understanding as to which legal basis will be used for the collection, storage and processing of the personal data being collected.
- b) which roles under the privacy accountable framework are accountable for implementing any required activities needed to be compliant with the lawful basis.

5. Determining Lawful Basis within Convatec

Prior to processing personal data, the lawful basis must be determined and be documented in a [Convatec Privacy Risk Assessment](#) (OneTrust -as part of the processing activity). This activity should be performed in conjunction with the [Information Asset Custodian] and with the guidance of the [Data Privacy Compliance Manager] as set out in the PAF.

Once you begin processing personal data under a specific lawful basis, you may not change the lawful bases to another basis to suit your purpose. For example, if explicit consent has been withdrawn by the data subject, it is not possible to use another lawful basis (e.g., not permitted to use legitimate interest) to continue to process the personal data.

If your purpose for processing changes at any point within the processing, a new lawful basis must be determined, approved, and documented.

Convatec primarily relies on obtaining explicit consent as its lawful basis for processing personal data. However, there are times where it is not feasible to collect explicit consent, or another lawful basis is more appropriate.

For each processing activity conducted within Convatec, one of the six (6) lawful basis (explained below) must be selected and documented within the Convatec Privacy Risk Assessment. Depending on the lawful basis selected, additional requirements may be required. See [Annex 3 for the Marketing and Sales Lawful Basis strategy](#)

Personal information may only be processed after the Privacy Risk Assessment has been approved. For questions related to lawful basis, please contact the Central Privacy team at dataprivacy@convatec.com.

6. Lawful Basis Types

a. Explicit Consent

Explicit Consent should be used as the lawful basis when you can offer a data subject a real choice and control over how their data will be used. If you cannot offer a genuine choice, explicit consent would not be an appropriate legal basis. (If explicit consent is a precondition of a service, it is unlikely to be the most appropriate lawful basis). For more information on explicit consent, please see Annex 2 - Rules for Consent.

To be valid, explicit consent must be freely given and specific, it must be an informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signifies agreement to the processing of their personal data.

When using explicit consent as a lawful basis, the request for explicit consent must be prominent, concise, separated from other terms and conditions, and easy to understand. It must include the following:

- The name of our organisation.
- The name of any third-party controllers who will rely on the explicit consent to collect, process, store, or share personal data;
- The specific reason(s) why you need the personal data;
- What you will be doing with the personal data (i.e., privacy notice); and
- How an individual may withdraw their explicit consent, at any time.

For example, the Ostomy Care Me+ patient support program asks participants for their Explicit Consent at the time of enrolment. If the participant does not opt-in to receiving marketing information from Convatec, the participant's data must not be processed for marketing activities within Convatec.

b. Performance of a contract

Performance of a contract should be selected as a lawful basis when you have contracted with the individual and the processing of personal data is necessary to comply with delivering the contractual service. This legal basis may also be applied when a data subject has asked you to do something as a first step (e.g., provide a quote).

Performance of a contract may not be used as a legal basis if the contract is held with another party, or the data subject's personal data will be reused for our own business purposes.

For example, Convatec sells ostomy products via its Ostomysecrets website. When a customer buys a product, we process the customer's personal data such as name, payment card details, billing and shipping address, etc. to fulfil the customer's order.

c. Legal obligation

Legal obligation may be selected as a lawful basis when the processing of personal data is required to comply with a common law or statutory obligation. The processing of personal data must be necessary to comply with the regulatory requirement.

For example, Convatec is required to comply with medical device safety regulations in markets in which we operate. An example is where such regulations require organisations that manufacture medical devices to implement the appropriate level of traceability around the use and supply of their medical devices.

This typically involves collecting personal data so that organisations and regulators can identify potentially serious adverse events and device deficiencies and ensure that the appropriate corrective action is taken, including issuing a product recall, or notifying users of safety information.

d. Vital interest

Processing personal data to protect the **vital interests** of an individual may be selected as a lawful basis where the processing of personal data is needed in order to protect someone's life, or mitigate against a serious threat to a person, for example a child or a missing person.

For example, our Amcare Group Nursing team provides home visits for patients using our products. In the event, a nurse discovers a patient incapacitated or in distress, they may process personal data to get additional medical attention or help (i.e., local police) for the individual.

e. Public task

Public Task may be selected as a lawful basis where it is necessary to process personal data to carry out a task in the public interest or exercise an official authority.

For example, a government agency has statutory powers to conduct research about the online shopping habits of consumers. The agency asks retailers to share the personal data of a random sample of their customers to enable it to carry out this function. It explains that it will process the data under 'public task' once it receives the information.

As the retailers are not subject to the agency's statutory function, they cannot share the information based on the agency's public task. However, they may consider disclosing the information under another lawful basis, e.g., legitimate interests.

f. Legitimate Interest

Legitimate interest may be selected as a lawful basis where processing operations do not fit into any of the other lawful bases. If you are relying on the legitimate interest basis you need to identify your legitimate interest and balance these against the interests of the data subject. This must be done by conducting a **legitimate interest assessment (LIA)**. The assessment is broken up into three parts:

- Identify the relevant legitimate interest;

- Show that the processing is necessary to achieve it; and
- Balance it against the individual’s interest, rights, and freedoms.

If you satisfy the requirements of the LIA, legitimate interest may be used as the lawful basis for the processing.

The template for assessment can be obtained from the Central Privacy Team (dataprivacy@convatec.com), and the completed legitimate interest assessment must be stored in OneTrust to support the desired processing activities.

7. Primary processes activities within Convatec

The following chart provides an overview of lawful basis examples for collecting, storage and processing of personal data within Convatec. **The chart is provided for educational purposes only and not designed to be a complete list of all processing activities within Convatec.**

Process	Lawful basis	Examples
Any 'non face to face' direct (communication) marketing activities	Explicit consent	Email, Short Message Service (SMS) marketing activities, social media platforms (e.g., Facebook, Twitter, Instagram, WhatsApp, etc.)
Sales activities including lead qualification	Explicit Consent	Sales and clinical personnel making appointments with healthcare professionals (HCPs) (e.g., calls and in person meetings)
Product compliant handling	Legal obligation	Clinical contacting Convatec about a patient adverse reaction when using a Convatec product.
Improving our products and services	Explicit consent	Collection of Net Promoter scores, Customer feedback surveys Improving our products and services using data subjects' data (e.g., tracking cookies on web sites, using non anonymised health data to improve services). Recording telephone calls for training, education, and quality purposes.
Targeted advertisements on 3rd party web sites	Explicit consent	Uploading data subjects' details into social media sites so they receive adverts for our products and services.
Fulfilling a sample request	Explicit Consent	The lawful basis for fulfilling a request for a product sample is through contract fulfilment. Before samples are provided, we need to obtain individual explicit consent to be allowed to provide samples, as well as to provide Convatec with the means to use and share data for sample follow-up activities. This is especially important for HCPs that we collect explicit consent, as the lawful basis we would typically rely upon is legal obligation, and this does not cover processing activities related to providing samples.

		Where the provision of providing a sample, involves marketing, a marketing explicit consent must also be collected to account for communications that go beyond the sampling process. For examples, communications about Convatec approved retailers (e.g., 180 Medical U.S.) and their services or other Convatec product and related service offerings.
Retaining details of whom we have sent samples to in case of product recall / advice needs to be issued	Legal obligation	When we send a product sample or product to a consumer or HCP, we need to retain their details for the shelf life of the product, should we need to reach out and inform them of a product recall or issue product usage information.
Providing a service	Explicit consent	In some markets, Convatec offers some direct-to-consumer services, such as Prescription fulfilment, purchasing of products and services and providing services via Convatec clinics. We also provide online education platforms such as ConvaTeach and Convatec Academy. Such services should always use explicit consent.
Provide Information and guidance around our products	Explicit consent	Customer registration into ME+ Programme.
Providing personalised content via web sites and conferences.	Explicit consent	Conferences (virtual and in person), Virtual reality, product tours, and Q&A, standard marketing campaigns linked to interests. Using personas, information collected, recommendations, presentation to the user of custom content based upon interests (e.g., Showpad, branded web sites).

8. Lawful basis and information retention

The lawful basis selected primarily determines how long an organisation may retain personal data. Once an organization no longer has a lawful basis for processing personal data, it must be deleted in accordance with Convatec’s Information Retention Policy and Retention Schedule³.

Lawful basis	Retention period and explanation
Explicit consent	2 years from when it was last collected or renewed. This includes Explicit Consent for marketing activities as well as data processing as per the privacy notice. When Explicit Consent is withdrawn for data processing activities, it is automatically withdrawn for marketing activities at the same time.
Legal obligation	There are many business processes where personal data needs to be retained for prolonged periods due to legal obligations, and these are set out in Convatec’s information retention policy and retention schedule ³ . Medical Device Safety Regulations A common regulatory obligation is the retention of personal data to meet requirements of medical device legislation, i.e. to

	<p>retain personal data of data subjects to whom we provide products to, so if needed, they can be contacted when safety advice needs to be circulated or recalls need to occur (5 years / Shelf life of Convatec products). The system of record for this data (where this data must be stored and retained) is SAP.</p> <p>When patients and HCPs contact Convatec regarding adverse effects and events with our products and services, we have an obligation to share this data with regulatory bodies when certain criteria are met, as well as retaining details for 25 years under medical device regulations across the USA and Europe. The system of record for this data is Trackwise.</p> <p>Fraud prevention regulations</p> <p>When we collect personal data for uses in sales processes in which commission is paid, As the principal reason for retaining personal data is the prevention and detection of fraud, the retention period for personal data collected for the prevention of fraud is 15 months from the last time there was either a face to face or telephone interaction with the data subject which is related to Convatec’s products and services (15 months comprises of 1 financial year plus 3 months for external auditors to certify company accounts).</p> <p>Note: Data may be retained for a minimum of 15 months and for as long as we continue to have Explicit Consent from the data subject (i.e., HCP).</p> <p>The system of record for this data is CRM.</p>
--	---

a. Exception to the rule

- i. **Do not contact:** On occasions, data subjects may request that Convatec no longer contact them or use their data. In such cases, Convatec will either delete all data belonging to the data subject where possible or tag their data so that systems and employees know not to contact / use. A do not contact flag shall remain in place for 5 years, unless explicit consent is renewed by the HCP. Convatec will retain all explicit consent and flag information for 5 years.
- ii. **Request my data is deleted:** Data subjects may also request that their data is deleted from our systems. Whilst this may be possible where we rely upon explicit consent, where there is a legal obligation to retain their data (i.e., legal obligation on Convatec to retain the data for a prolonged period) we would keep the data for this period of time. Typically, we would delete data or ‘put out of use’ from CRM upon request, but not from systems like SAP or Trackwise.
- iii. **HCPs and Clinicians:** Convatec obtains details of clinicians and HCPs through a variety of sources, including in the public domain. Where a data subject wants their data to be deleted from our systems, the data subject must be given a choice on how their data request should be managed by Convatec. They can choose to have it deleted or marked with a “do not contact” flag. If Convatec has interacted with the data subject regarding our products and services, we are obliged to retain their data for a period of 15 months from the interaction date. Regardless of the data subject’s choice, we may still come across their details again in the public domain. There may be a situation where there is a need for Convatec to re-engage them which will require Convatec to obtain explicit consent.

9. Terminology

Term used	Explanation of term
Data subject	A person, in the case of this document data subjects could be patients or clinicians (e.g., Health care professionals).
HCP	Health care professional / clinician.
Personal Data	Any information relating to a person (a 'data subject') who can be identified, directly or indirectly, this includes identity data (e.g., Name, address, date of birth, identification numbers, health or financial data), usage data, and other data belonging to patients / and or clinicians.
Processing	In relation to personal data, means any operation or set of operations which is performed on personal data or on sets of personal data (including: whether by automated means, such as collection, storing, processing, disclosure, erasure, or destruction).
reCAPTCHA	reCAPTCHA is a system that enables web hosts to distinguish between active human selection and artificial intelligence selection programs. The system is used to prevent the misuse and abuse website access. The original version asked users to decipher hard to read text or match images in order to gain access to the desired website.
special category data	Personal data that needs more protection because it is sensitive. e.g., personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data.
criminal offence data	Any personal data which is linked to criminal offences, or which is specifically used to learn something about an individual's criminal record or behaviour.

10. Contact Information and Quality System:


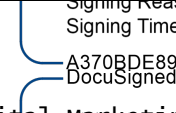
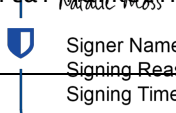

This document is owned by: Convatec Information Technology Function

Annex 1 - History and Approvals

History

VERSION: V.01	ORIGINATOR: James Osijo Laura Caravetta	DATE: 07-07-2023
COMMENTS: CONVATEC NEW ENTITY ISSUE		
TRAINING REQUIRED? (Always required for original/ver. 1.0 documents)	<input checked="" type="checkbox"/> YES (Indicate minimum requirements needed before document is effective)	<input type="checkbox"/> NO (Indicate Why Not): Minor updates to document. Effective documents will be communicated in accordance with Document Control procedures for completion as read and understood.

Approvals

Name	Job Title	Signature	Date
Andy Hunter	Global SFE CRM Sales Enablement Director	 DocuSigned by: Andy Hunter Signer Name: Andy Hunter Signing Reason: I approve this document Signing Time: Oct 5, 2023 5:54:49 PM BST	Oct 5, 2023
Natalie Moss	Global Director of Digital Marketing (MCoE)	 DocuSigned by: Natalie Moss Signer Name: Natalie Moss Signing Reason: I approve this document Signing Time: Oct 5, 2023 4:34:11 PM BST	Oct 5, 2023
James Osijo	Head of Privacy & Group Data Protection Officer	 DocuSigned by: James Osijo Signer Name: James Osijo Signing Reason: I approve this document Signing Time: Oct 5, 2023 6:40:00 PM BST	Oct 5, 2023
Laura Caravetta	Senior Privacy Officer, Americas	 DocuSigned by: Laura Caravetta Signer Name: Laura Caravetta Signing Reason: I approve this document Signing Time: Oct 5, 2023 6:35:46 PM BST	Oct 5, 2023

Annex 2 - Explicit Consent Rule

1. Collecting Explicit Consent

Explicit consent must be collected for each distinct purpose we want to use the data subject's data for. This means that explicit consent must be collected for the collection, storage and processing of their personal data in accordance with our privacy notice. For example, if we are providing samples to a data subject, and we would like to market to them, we must also collect marketing explicit consent from the data subject.

2. Cookie Explicit Consent

Website technologies which are used to track individuals, using cookies or similar technologies are subject to consent. Any cookies or similar tracking technologies which are 'non-essential' or not strictly necessary to make a website work must require explicit consent before cookies are dropped on to the data subjects' device.

3. Explicit Consent Template

When relying on explicit consent (i.e., marketing, cookie, etc.), explicit consent language must be reviewed and approved by the Central Privacy Team. Please visit for [Convatec's Data Centre](#) for approved explicit consent templates. If you have questions or need more information, please contact the Central Privacy team at dataprivacy@convatec.com.

4. Storage of explicit consent for data processing and marketing

Where we know who the data subject is (e.g., sales and marketing processes), explicit consent is to be stored in Convatec's Consent management platform (OneTrust). Explicit consent may also be stored in systems such as CRM, but these must be kept in sync with the consent management platform.

5. Demonstrating that the data subject has provided consent

When using explicit consent as the lawful basis, Convatec must be able to demonstrate that a data subject has provided consent. Convatec may use phone recordings with the data subject or emails, SMS, or mail from the data subject e.g., double opt-in to demonstrate and verify that the data subject has given consent.

It is Convatec's policy that all new solutions which collect explicit consent must be integrated into Convatec's Consent management platform OneTrust (this allows Convatec to evidence collection of consent). Convatec requires that a data subject double opt-in to the activity they are providing consent. An individual may double opt-in by providing consent and using a second method to demonstrate it is themselves (i.e., email or text verification).

Evidence that data subject has provided consent must be retained for the entire time that the consent is being relied on. Documenting that a data subject provided consent within the system without evidence is not sufficient for demonstrating that a data subject provided consent.

6. Renewing consent by channel

A data subject's consent must be renewed every two (2) years or if any of the following occur:

- Purpose of processing changes - if you plan to use the user's personal data for another purpose that was not previously shared
- Changes in personal data collected- if there are changes to the type of personal data you are collecting or processing
- Legal/regulatory changes- if the applicable laws or rules regulating data protection and privacy change

Channel	Examples	Suggested follow on activities
Face to Face	In person sales meetings	If required, we should confirm consent given / renewed and offer to send a summary including link to the appropriate privacy notice.
Telephone	Scheduled customer calls	Send them a link (e.g., SMS) to the OneTrust consent and preference centre when changes are made to consent or record and document on a call.
Digital (email)	'Scheduled privacy check-up' campaign	Send them a link (e.g., email) to the OneTrust consent and preference centre when changes are made to consent.
Mobile and web applications	Data subject changes preferences in mobile app or in OneTrust consent centre	If a user was authenticated to our systems, although not necessary, you can send a confirmation email thanking them for reviewing their privacy settings....

1. Communication and marketing channels

When we collect consent for marketing activities, it is appropriate to assume based upon the channel and contact information that we can market to the data subject (i.e., patient, HCP, customer) via those channels. For example, if we collect an email address when collecting marketing consent on a web form, then from a preference perspective it is safe to assume they are opting into email marketing. If we collect contact information not at the time of collecting consent (e.g., product support, inquires, providing a sample), it does not automatically mean that the data subject is expressing a preference that they want to receive direct marketing via that channel, unless we ask the data subject at the time.

2. Providing options not to collect personal data when we don't have consent

Consent must be given freely; therefore, services must be designed so that they do not collect personal data without consent. For example, Customer interaction centres should have a mechanism not to record telephone calls (e.g., 'This call is being recorded for quality and training purposes; if you would rather this call, not be recorded press 9 now) and web chats must seek consent before recording the content of web chats.

Annex 3 - Marketing and Sales Lawful Basis strategy

Collection Purpose	Consent To	Data Subject	Constraints	Consent Valid For	Processing Purpose	Related Processes	Lawful Basis	Comms	Notes
Me+ Programme	Use of Data	Patient	Mandatory	2 years	Promotion of free to use services; Telehealth appointment, counselling, community	Me+ registration (via phone)	Explicit Consent	Email, Telephone call	If comms includes any reference to products, it is deemed direct marketing
					Send the customer information pertinent to their medical condition e.g., ostomy recovery series	Service comms	Explicit Consent	Email	
					Contact customer to conduct a telehealth appointment	Fulfilment of telehealth request	Explicit Consent	Telephone call	
					Contact customer to provide counselling session	Fulfilment of counselling request	Explicit Consent	Telephone call	
					Sending a customer survey	Improving products and services	Legitimate Interest	Email	Survey communication may be sent once to any customer who has taken affirmative action within the past six months
					Customer Survey	Improving products and services	Explicit Consent	Survey	Explicit consent must be obtained prior to the collection of survey data
					Recording telephone calls for training, education, and quality purposes	Improving products and services	Explicit Consent	Telephone Call	

Collection Purpose	Consent To	Data Subject	Constraints	Consent Valid For	Processing Purpose	Related Processes	Lawful Basis	Comms	Notes
					Patient education as support (not product related) e.g., getting back to exercise tips	Service comms	Explicit Consent	Email, Mail	If comms includes any reference to products, it is deemed direct marketing
Sample Request	Use of data	Patient or HCP	Mandatory	2 years	Contact the customer to qualify the sample (right products to send)	Fulfilment of sample request	Explicit Consent	Telephone call	
					Contact the customer to gather more information about their circumstances e.g., products in use	Fulfilment of sample request	Explicit Consent	Telephone call	
					Sending the sample to the customer	fulfilment of sample request	Contract fulfilment	Telephone call	
					Sharing product information (e.g., user guides)	Service comms	Explicit Consent	Email	
					Contact the customer to verify sample received	fulfilment of sample request	Explicit Consent	Telephone call	
					Contact the customer to gather feedback on the sample used	Improving products and services	Explicit Consent	Telephone call	
					Recording telephone calls for training, education, and quality purposes	Improving products and services	Explicit Consent	Telephone Call	
					Contacting customer in regard to product recall	Product recall	Legal obligation - medical device safety regulation	Email, Mail, telephone call	
Retail Referral	Retailer Referral	Patient	Optional	2 years	Contact the customer to discuss product supply options	Marketing comms, Fulfilment of sample request	Explicit Consent	Telephone call	

Collection Purpose	Consent To	Data Subject	Constraints	Consent Valid For	Processing Purpose	Related Processes	Lawful Basis	Comms	Notes
					Sending data onto 3rd party for purpose of setting up a product supply	Fulfilment of sample request	Explicit Consent	Telephone call	
Direct Marketing	Direct Marketing	Patient or HCP	Optional	2 years	Promotion of events or webinars	Marketing comms	Explicit Consent	Email, SMS	
					Promotion of products and samples	Fulfilment of sample request, me+ registration (Via phone)	Explicit Consent	Email, SMS Telephone call, Mail	
					Promotion of partnered retailers; Ostomy Secrets, 180 Medical, etc.	Marketing comms, Fulfilment of sample request, me + registration (Via phone)	Explicit Consent	Email, SMS Telephone call, Mail	
					Share news about Convatec and its partners/affiliates	Marketing comms	Explicit Consent	Email, Mail	
					Promote loyalty Programmes e.g., Me +	Marketing comms, Fulfilment of sample request	Explicit Consent	Email, SMS, Telephone call, Mail	
Sample request via SFE	Use of date	HCP	Inferred	N/A	Sending a sample to practitioner/Giving it in person	Fulfilment of sample request	Legal obligation data	Telephone call	
					Contacting practitioner to verify sample has been received	Fulfilment of sample request	Legal obligation: Fraud prevention	Telephone call	

Collection Purpose	Consent To	Data Subject	Constraints	Consent Valid For	Processing Purpose	Related Processes	Lawful Basis	Comms	Notes
					Contacting practitioner in regard to product recall	Product recall	Legal obligation: Medical device safety regulation	Email, Telephone call	
Product demonstration or consultation with sales agents (SFE)	Use of data	HCP	Inferred	N/A	Record interaction with HCP	Sales consultation	Legal obligation: Fraud prevention	Face to Face, Telephone call	
				N/A	Lead qualification	Lead qualification	Legitimate interest	N/A	
				N/A	Recommended products and samples based on problems discussed with current	Sales comms	Legitimate interest	Face to Face, Email, Telephone call	
				N/A	Informing about back orders or stock issues	Sales comms	Contractual obligation	Face to Face, Email	
				N/A	New formulary/tender listing impacting their treatment or care decisions	Sales comms	Legal obligation	Face to Face, Email, Telephone call	
				N/A	Follow up on product complaint	Complaint procedure	Legal obligation - medical device safety regulation	Face to Face, Email, Telephone call	
			Mandatory	2 years	New Products / or services that will be beneficial to HCP and support existing patient treatment	Sales comms	Explicit Consent	Face to Face, Email, Telephone call	
			Mandatory	2 years	Sharing content via showpad based on existing discussion	Sales comms	Explicit Consent	Email	
			Mandatory	2 years	Changes to Product Indications or new insights / evidence in the marketplace	Sales comms	Explicit Consent	Face to Face, Email, Telephone call	

			Mandatory	2 years	Patient benefits and / or cost savings based on patient treatment protocols	Sales comms	Explicit Consent	Face to Face, Email, Telephone call	
			Mandatory	2 years	Follow up on HCP request/ items discussed in meetings	Support process	Explicit Consent	Face to Face, Email, Telephone call	
Collection Purpose	Consent To	Data Subject	Constraints	Consent Valid For	Processing Purpose	Related Processes	Lawful Basis	Comms	Notes
Contact us	Use of date	Patient or HCP	Mandatory	2 years	Contact customer regarding a complaint made	Complaint's procedure	Legal obligation	Email, Telephone call	
					Do not contact request	Do not contact	Explicit Consent		
					Contacting customer regarding a request to delete their data	Right to be forgotten	Explicit Consent	Email, Telephone call	
Webinar	Use of Data	HCP	Mandatory	2 years	Contact the customer with event information	Service comms	Explicit Consent	Email, Telephone call	
Clinical education and or training on appropriate product usage	Use of date	HCP	Inferred		Share information about the training and follow-up with training/education materials	Sales comms	Legit interest	Face to Face, Email, Telephone call	
Prescription Request	Use of Data	Patient	Mandatory	2 years	Confirm order	Service comms	Performance of a contract	Email	
					Call to confirm insurance details	Prescription fulfilment	Performance of a contract	Telephone call	
					Send customer updates on fulfilment (e.g., being processed, out for delivery, delivered)	Service comms	Performance of a contract	Email	
eCommerce (medical products)	Use of Data	Patient	Mandatory	2 years	Confirm order	Service comms	Performance of a contract	Email	
					Call to confirm insurance details	Product fulfilment	Performance of a contract	Telephone call	

					Send customer updates on fulfilment (e.g., being processed, out for delivery, delivered)	Service comms	Performance of a contract	Email	
eCommerce (non-medical products) e.g., ostomy secrets	Use of Data	Patient	Mandatory	2 years	Confirm order	Service comms	Performance of a contract	Email	
					Send customer updates on fulfilment (e.g., being processed, out for delivery, delivered)	Service comms	Performance of a contract	Email	
Collection Purpose	Consent To	Data Subject	Constraints	Consent Valid For	Processing Purpose	Related Processes	Lawful Basis	Comms	Notes
Educational information request - Papers, publications, product information (HCP only)	Use of Data	HCP	Mandatory	2 years	Send practitioner information or grant access to materials	N/A	Explicit Consent	Email	