2020

# GDPR Call Handling And Escalation Process

| REVISION | COMMENTS | AUTHOR | DATE |
|---|---|---|---|
| Rev 0.001 | Draft | Arlo Support Ops | |
| | Published | Arlo Support Ops | 1/20/2020 |
| | | | |
| | | | |
| | | | |

# Table of Contents

## PURPOSE

To define the process of handling calls from customers who are seeking information regarding the recent update on EU General Data Protection Regulation (GDPR).

## UNDERSTANDING GDPR AND PRIVACY

In May 2018 the EU General Data Protection Regulation (GDPR) replaces the existing patchwork of EU National Data Protection legislation and brings a level of consistency to data and privacy protection in the EU. Even prior to the implementation of GDPR, Arlo recognized the worldwide importance of privacy, security, and data protection to our customers, partners, and employees.

We have a cross-functional approach to privacy governance, which covers all areas of the company and includes customer, partner, and employee data. The legal, customer care, IT, HR and Engineering teams meet on a regular basis to help guide, design, and develop products and systems from the ground up to protect data and privacy. Arlo has a Board of Directors' Cybersecurity Committee that is tasked with the oversight and monitoring of Arlo's privacy and data security and regularly engages with outside experts regarding various privacy issues including privacy by design and encryption. Arlo has an active cybersecurity program and to make sure information is secure, we strictly enforce privacy safeguards within the company. This means we use access management and access controls commensurate with the risk to data to ensure access to data is associated with a business need, such as providing customers with support.

Specifically, as part of our EU General Data Protection Regulation (GDPR) work, we have assessed, and continue to assess, our major processes, products, and services. In particular, we have:

- Rewritten our privacy policy (https://www.arlo.com/en-us/about/privacy-policy/?cid=a)
- improved processes to help ensure data transparency, accuracy, accessibility, completeness, security, and consistency;
- mapped our data and identified what we have, what we are doing with it, where it is, where it flows, and who has access to it;
- assessed the privacy and data security risks and strengths in our enterprise systems and products;
- implemented data incident response teams and processes;
- implemented additional third-party controls, vendor oversight, monitoring, audit, and remediation requirements; and
- embedded privacy and security requirements in the product development cycle.

In addition, all Arlo employees are required to take training on Privacy and Security.
Finally, Arlo complies with all applicable laws that require notification about data security incidents. That means we conduct prompt investigations and analysis, so that we can provide notification in a timely manner if necessary. We are also committed to providing customers that have been impacted by an incident with appropriate assistance, which may include information about support from Arlo or advice on steps customers can take to reduce the risk of harm.

## L1/L2 RESPONSIBILITY

- If the customer is calling regarding whether Arlo is GDPR compliant,
    - Expert must refer the customer to GDPR statement above AND to the updated Private Policy which can be found in https://www.arlo.com/en-us/about/privacy-policy/?cid=a
    - Expert can also forward this statement in written to the customer OR link to it, but it **MUST NOT** be modified since we need to be sure we can honour any commitments we make in the statement.
    - If the customer is asking about whether Arlo is GDPR compliant, expert's spiel should be:

***"Mr. Customer, as GDPR is very broad regulation, I will follow up with you in written referring you to Arlo Private Policy and GDPR statement. Should you have any further questions afterwards, do not hesitate to contact us again at any stage."***

    - Experts must **refrain** from saying, YES, Arlo is GDPR compliant.
    - Such case **does not** need to be escalated to CCT, UNLESS customer follows up and is asking any extra questions about GDPR and compliance.

Meanwhile, if the customer is calling in relation to the account deletion, subject access, correction of inaccuracies, request to the processing of information or data portability request, **escalate such case to CCT**.

## CCT RESPONSIBILITY

Once CCT receives the escalation, they are required to take ownership of the case and ensure that all details regarding the concern is documented and logged on the case.

CCT must identify what the GDPR request is about. Depending on the issue, CCT will take the next action to complete the request.

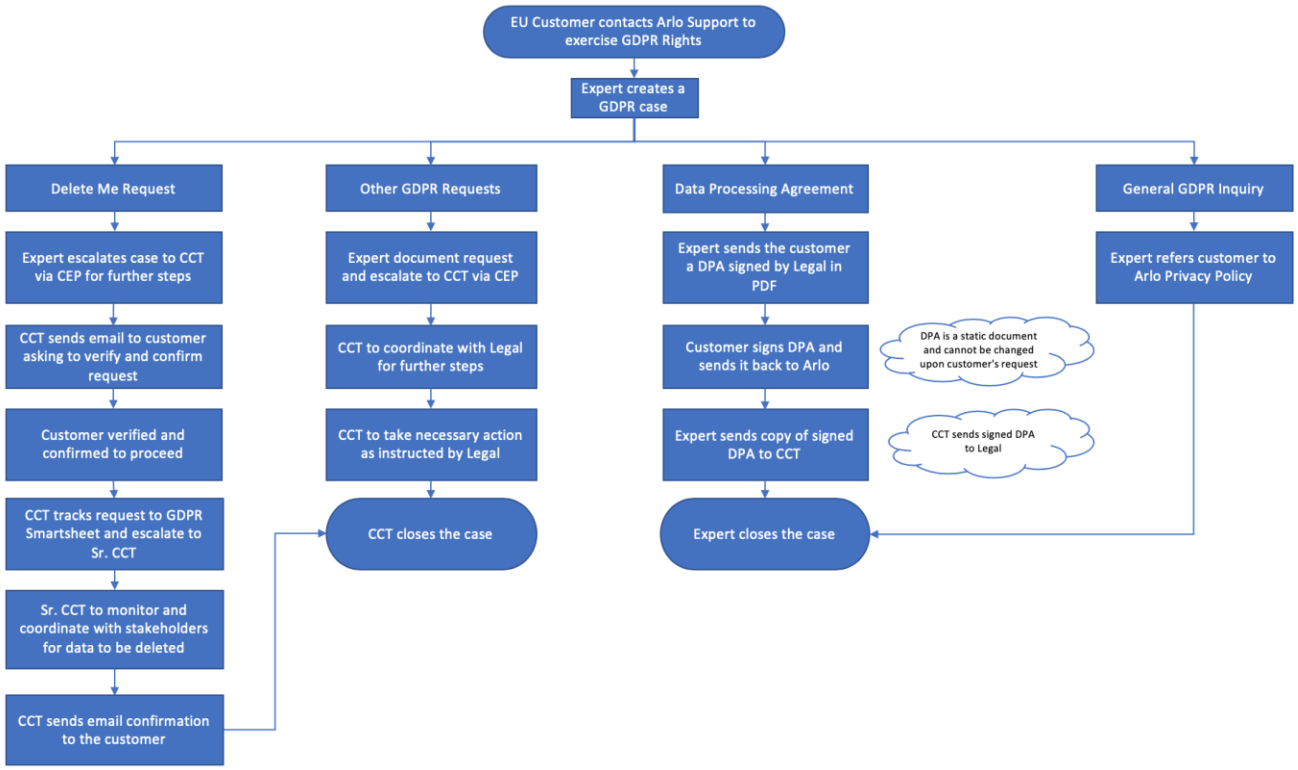
1. **DPA Request/Delete Data Records/Request for Data**
    - CCT to send an email to expert containing a PDF version of the DPA signed by Legal
    - CCT to remind expert that the said file is a static document and the customer can either agree or refuse to sign
    - CCT to advise expert to return signed copy from the customer
    - CCT to send email to Legal along with the signed DPA from the customer

2. **Other GDPR Inquiry**
    - When CCT receives an escalated case from the expert which contains specific GDPR requests such as Subject Access Rights, Inaccuracies needing correction or disputes from our current Privacy Policy, etc. – CCT identifies GDPR rights being exercised and summarizes issue
    - Once issue has been fully understood, CCT sends email to Legal seeking help on how to proceed or how to respond

- Depending on the instructions from Legal, CCT will proceeds to the next steps.

3. **Delete Me Requests**
   - When CCT receives escalated case regarding Delete Me requests, CCT reviews case disposition to ensure GDPR Approval process is triggered in CEP
   - If the GDPR approval process is not triggered due to incorrect selection of CEP tagging, CCT deescalates support case and creates a new CEP case
   - CCT sends an email to the customer asking to verify their identity and confirm they wish to proceed with the request
   - Once customer responds and confirmed to proceed, CCT tracks the GDPR case in SmartSheet
   - A Sr. CCT advocate regularly checks GDPR tracker to ensure that requests are completed before the 30day mandate
   - Sr. CCT follows up with CEP approvers for data to be masked in CEP
   - Once CEP data is masked, Sr. CCT then masks Aria billing details
   - When CEP and Aria data is masked, Sr. CCT reaches out to Jay Sudhakar to delete the customer's xCloud ID which will prevent the customer to login to their Arlo account
   - After the customer's account is deleted, the next step is to check if the customer has any Arlo community account which goes to Community Team (James Cross).
   - Once all the steps above is completed, CCT sends an email confirmation to the customer and closes the case.

## ARLO GDPR PROCESS FLOW



## ARLO DELETE ME PROCESS FLOW

**Customer Support**

- Expert receives Delete Me request from EU Customer
- Expert creates a Delete Me case to trigger approval process and escalates case to CCT
- CCT sends email to customer asking to verify request and confirmation to proceed
- CCT tracks case details to Smartsheet and follow up on other stakeholders

**CEP**

- Once GDPR Delete Me case disposition is selected, a GDPR Approval process is triggered
- Approvers starts from Legal then goes to Finance, Operations (2 levels) and finally IT
- When all the departments submit their approvals, the customer contact details get masked in CEP

**Aria (Billing)**

- When CEP data is masked, Aria (billing) details is next to be masked
- CCT accesses customer's Aria account and remove any active plans
- CCT to process refunds, if any
- CCT removes card details
- CCT masks customer account information by changing customer details to 'xxxxxxx'

**xCloud ID**

- CCT emails Jay Sudhakar to send list of email addresses with masked CEP and Aria details
- Jay sends email to his team who creates CR for xcloud ID to be deleted
- Once xCloud ID is deleted, customer will no longer be able to login to their Arlo account

**Lithium (Community)**

- The next step after xCloud ID deletion is to deactivate community accounts of the customer, if any
- CCT sends an email to James Cross for help in locating any community account related to the email and deactivate it

## SAMPLE GDPR TRACKER IN SMARTSHEET

| Case Number | Customer Name | Email Address | GDPR Request Type | Date Customer Confirmed | Customer Verified (Customer Respond... to Proceed) | CEP Data Masked | Aria Billing Details Removed | Removed from XCloud | Removed from Lithium (Khoros) | Delete Completion Date | Within 30 Day Mandate | Case Status |
|---|---|---|---|---|---|---|---|---|---|---|---|---|