



Data Sharing and Tracing Solutions for the Public Sector

LoCTA Hub GDPR Compliance Policy

This document, and any implied design, is the copyright of LoCTA Ltd. It may not be reproduced in whole or in part by any means without written consent of LoCTA Ltd. LoCTA Ltd. cannot be responsible for the accuracy or validity of any data retrieved from any Local Authority system.

CONTENTS

Change Control.....2

GDPR and LoCTA Ltd for LoCTA.....3

LoCTA Ltd Policy for Processing Data.....4

 To ensure GDPR compliance LoCTA Ltd will:.....4

 Our Direct Responsibilities under GDPR are to:.....4

 LoCTA Ltd policy for controlling data5

 Subject access requests5

 What LoCTA Ltd will do should there be a data protection breach5

Change Control

Version	Date	Description	Author
1.0	May 2018	Initial Draft	TC
1.1	Feb 2020	Updated to LoCTA Hub / LoCTA Ltd	TC
1.2	Feb 2022	Updated Data Hosting text	TC
1.3	March 2023	Updated with DPO / Article 9 details	TC

GDPR and LoCTA Ltd for LoCTA Hub

The intention of the GDPR is to strengthen data protection for individuals within the European Union and become enforceable on 25 May 2018.

LoCTA Hub Data Privacy Impact Assessment

LoCTA Ltd contracted an external recognised GDPR expert to complete a comprehensive DPIA (Data Privacy Impact Assessment) for the LoCTA application and service.

Our obligations as a processor & Lawful Basis for processing

Under UK GDPR, data protection principles set out the main responsibilities for organisations and the need to identify a lawful basis before processing personal data.

Consent is not required by Local Authorities, County Councils or Central Government Agencies for using LoCTA Hub in their duties to protect the public purse and the relevant sections are listed below.

Specific Provisions in UK GDPR and DPA2018 Overview

Article 6 Lawfulness of Processing

6(1)c Processing is necessary for compliance with a legal obligation

6(1)e Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

Article 9 Processing of Special Categories of Personal Data

9(2)g Processing is necessary for reasons of substantial public interest

Part 2 of Schedule 1 DPA2018

- 10. Preventing or detecting unlawful acts
- 11. Protecting the public
- 14. Preventing Fraud
- 15. Suspicion of Terrorist Financing or Money Laundering

Specific Provisions in UK GDPR and DPA2018 Detail

These are detailed in full, in our Customer Data Sharing Agreement.

Data Hosting, Data Retention & Accuracy of Data

As your data is stored on our IT infrastructure, and shared with our data processors, it may be transferred and stored securely outside the European Union. Where that is the case it will be subject to equivalent legal protection through the use of Model Contract Clauses.

Our Data Retention policy adheres to strict controls. Contractual requirements between LoCTA Ltd and each Local Authority Data Controller client mandates that the data sets are refreshed weekly. There are policies in place to manage this. All data files received are securely shredded at 28 days, and backups held for 3 months.

Should any data be reported by the Local Authority Data Controller as inaccurate, LoCTA Ltd have policies in place to adhere to the GDPR principles and resolve this with the Data Controller within the mandated guidelines.

LoCTA Ltd Policy for Processing Data

To ensure GDPR compliance LoCTA Ltd will:

- only act upon written instructions of our clients (normally Local Authorities as the data controllers)
- be subject to a duty of confidence, and ensure the same of all relevant staff members
- ensure the appropriate measures are taken to ensure the security of the processing.
- only engage a sub-processor on written consent of the data controller
- assist the data controller in providing subject access and allowing data subjects to exercise their rights under the GDPR
- 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
- ensure to delete or return all personal data to the controller as requested at the end of any relevant contracts
- submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 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.
- train our staff to comply with these regulations

Our Direct Responsibilities under GDPR are to:

- only act on the written instructions of the controller (Article 29);
- not use a sub-processor without the prior written authorisation of the controller (Article 28.2);
- co-operate with supervisory authorities (such as the ICO) in accordance with Article 31;
- ensure the security of its processing in accordance with Article 32;
- keep records of its processing activities in accordance with Article 30.2;
- notify any personal data breaches to the controller in accordance with Article 33;
- employ a data protection officer (DPO) if required in accordance with Article 37; and
 - we are not required to have a DPO. We do have a specified Data Protection contact, who monitors our compliance with the UK GDPR and other data protection laws, updates our data protection policies, raises awareness of data protection issues, monitors team training, advises and monitors DPIAs and would be the first point of contact for the ICO and for individuals whose data is processed.
- appoint (in writing) a representative within the European Union if required in accordance with Article 27.

LoCTA Ltd policy for controlling data

To ensure GDPR compliance LoCTA Ltd will:

- only collect & retain information necessary to transact with our customers and prospects
- ensure that revoked consent requests are managed with 48 working hours of revocation
- ensure to enable right to access within 7 days of request, unless otherwise specified in writing.
- train our staff to comply with the regulation

Subject access requests

Upon receiving a written subject access request LoCTA Ltd will:

- on the rights of Access/Erasure/Correction, will refer to the relevant Local Authority Data Controller and will engage with the Data Controller as necessary to fulfil these requirements
- ensure to verify the identity of the person requesting the information
- respond in writing within 40 calendar days with the requested information
- if requested, initiate the right to erasure process

What LoCTA Ltd will do should there be a data protection breach

Should there be a data breach, staff are trained to inform their line manager immediately, who will in turn, inform an authorised member of personnel at the client and also inform the ICO within 24 hours.

The information provided to the client and the ICO will include;

- What has happened;
- When and how we found out about the breach;
- The people that have been or may be affected by the breach;
- What we are doing as a result of the breach

The management team at LoCTA Ltd are responsible for the compliance and maintenance of this policy