# UDCLT UK GDPR Article 30 Inventory - Marketing

| 1. Project Overview | |
|---|---|
| **Name of the product, process, service, application, or system ("Project")**[1] | Managing marketing information |
| **Brief description of the Project** | Communicating generally with donors, interested parties, mailing lists and website visitors |
| **The UDCLT legal entity responsible for the Project ("Business")** | The Upper Dales Community Land Trust (Company and Charity) |
| **The UDCLT Contact Details** | udcltrust@gmail.com |

| 2. Data Controller or Data Processor (Internal Use Only) | |
|---|---|
| **Does the UDCLT operate this Project on its own behalf (as a "data controller"[2]) or as a service provider to its customers (as a "data processor"[3])?** | Solely as a data controller |

| 3. The UDCLT as Data Processor (Complete these Questions Only if the UDCLT is Acting as a Data Processor—See Question 2) | | |
|---|---|---|
| **If the UDCLT is acting as a data processor, which the UDCLT database/system identifies the names and contact details of these customers?** | n/a | |
| **What types of data processing activities does the Project perform?** (check all that apply) | ☐ | Collection |
| | ☐ | Recording |
| | ☐ | Organisation |
| | ☐ | Structuring |
| | ☐ | Storage |
| | ☐ | Adaptation or alteration |
| | ☐ | Retrieval |
| | ☐ | Consultation |

[1] This form should be filled in for each processing activity that the UDCLT undertakes (such as processing of employee data, processing of beneficiary data etc. or if the UDCLT decides to implement new systems, applications, procedures or projects).

[2] A data controller is a party which, whether alone or jointly with others, determines the purposes and means of the processing of personal data.

[3] A data processor is a party which processes personal data on behalf of a data controller.

| | | |
|---|---|---|
| | ☐ | Use |
| | ☐ | Disclosure by transmission, dissemination, or otherwise making available |
| | ☐ | Alignment or combination |
| | ☐ | Restriction, erasure, or destruction |
| | ☐ | Other (please specify): _____ |

| **4. The UDCLT as Data Controller (Complete these Questions Only if the UDCLT is Acting as a Data Controller—See Question 2)** | | |
|---|---|---|
| **About which categories of individuals is personal information collected or otherwise processed?** (check all that apply) | ☐ | Company employees (including former employees) |
| | ☐ | Company job applicants |
| | ☐ | Company volunteers |
| | ☒ | Individual customers (consumers or owners or sole proprietary businesses) |
| | ☒ | Donors |
| | ☒ | Company beneficiaries |
| | ☐ | Representatives of business partners |
| | ☐ | Visitors of company premises |
| | ☒ | Visitors of websites/online |
| | ☐ | Persons entered into a company corporate register or list (e.g., shareholders) |
| | ☒ | Survey respondents |
| | ☐ | Children under the age of 16 |
| | ☒ | Other (please specify): mailing list sign-ups |
| **What types of sensitive/special personal information are collected or otherwise processed?** (check all that apply) | ☐ | Health & wellbeing information (physical or mental, such as disabilities, smoking habits, health / sporting activity surveys) |
| | ☐ | Medical information |
| | ☐ | Biometric data (fingerprints, iris scans) |
| | ☐ | Genetic data |
| | ☐ | Photos/videos/images used for identification or authentication of an individual |
| | ☐ | Racial or ethnic data |
| | ☐ | Religion and philosophical beliefs |
| | ☐ | Trade union membership |
| | ☐ | Political opinions or beliefs |
| | ☐ | Sexual orientation/sex life |
| | ☐ | Criminal records or information about criminal/unlawful behavior |
| | ☐ | Precise geo-location data (such as GPS-level data) |

| | | |
|---|---|---|
| | ☐ | Government issued identifiers (e.g. social security number, driver' license number, passport number) |
| | ☐ | Camera recordings of individuals in public spaces or publicly accessible spaces |
| | ☐ | Other (specify): photos for publicity purposes |
| **What other (non-sensitive) types of personal information are collected or otherwise processed?** (check all that apply) | ☒ | Contact information (such as name, address, email, phone) |
| | ☐ | Work contact information (name, address, email address, phone) |
| | ☐ | Marital Status |
| | ☐ | Gender Identity |
| | ☐ | Education and training history (such as CVs, degrees, titles, work permits) |
| | ☐ | Transaction history (such as purchased products and services) |
| | ☒ | Financial account information - only card type |
| | ☒ | Electronic identification data (such as IP, cookies, logs, online surfing facts) |
| | ☐ | Household characteristics (such as number of dependents, residence permits, rented / purchased, duration) |
| | ☐ | Employee ID |
| | ☐ | Employee disciplinary records |
| | ☐ | Employee performance rating/evaluation |
| | ☐ | Salary |
| | ☐ | Pensions and benefits |
| | ☐ | Age or birthdate |
| | ☐ | Insurance data |
| | ☐ | Vehicle data (such as license plate number, telematics data, etc.) |
| | ☐ | Beneficiary and emergency contact information |
| | ☐ | Other (specify): Whether you're gift aid registered, donation amount, date of last donation, donor message and/or reason for fundraising (if one is left) |
| **What categories of recipients will receive or have access to the personal information?** (check all that apply) | ☒ | Company |
| | ☒ | Company's third party service providers/vendors (e.g. donation platforms) |
| | ☐ | Regulators |
| | ☐ | Business partners |
| | ☐ | Auditors and professional advisors, such as lawyers and consultants |
| | ☐ | Law enforcement officials |
| | ☐ | Other (specify): _____ |
| **For what purposes is the personal** | ☒ | Contacting donors or supporters |

| | | |
|---|---|---|
| **information collected or used?** (check all that apply) | ☒ | Processing customer/donor/supporter requests |
| | ☐ | Internal investigations |
| | ☐ | Enforcement of policies |
| | ☐ | Human Resources purposes (such as recruiting, hiring, managing employment relationships) |
| | ☐ | Developing new products or services |
| | ☐ | Managing commercial relationships (such as invoicing, contract management) |
| | ☒ | Provision of products/services to individual customers |
| | ☒ | Data analysis not aimed at individual level (e.g., trend analysis) |
| | ☐ | Data analysis or profiling of the individual |
| | ☐ | To make automated decisions about the individual (e.g. screening of employment applications, customer acceptance, etc.). |
| | ☒ | Marketing (non-targeted/non-personalized) |
| | ☒ | Targeted and/or personalized marketing |
| | ☒ | Other (specify): collecting donations and gift aid, thanking donors |
| **On what lawful basis is the personal information collected or otherwise processed?** (check all that apply) | ☒ | Consent – the individuals have given consent for the UDCLT to process their data for one or more of the purposes listed above |
| | ☐ | Contract – the processing is necessary for a contract that the UDCLT has with the individuals concerned |
| | ☐ | Legal Obligation – the processing is necessary for the UDCLT to comply with the law |
| | ☐ | Vital Interests – the processing is necessary to protect the vital interests of the individuals concerned or another person |
| | ❒ | Public Task – the processing is necessary for the UDCLT to perform a task in the public interest, and the task or function has a clear basis in law |
| | ☒ | Legitimate Interests - the processing is necessary for the UDCLT's legitimate interests or the legitimate interests of a third party e.g. processing donations |
| **For what period of time will the personal information be retained?** (If different time periods apply to different categories of personal information, please specify each.) | ☐ | 2 months |
| | ☐ | 6 months |
| | ☐ | 12 months |
| | ☐ | 24 months |
| | ☒ | 5 years we can anonymize it after this time but before so that we can contact you if you've signed up for marketing, so we can process donations |
| | ☐ | Other (specify): _____ |

| 5. Data Transfers to Recipients in Other Countries | | |
|---|---|---|
| **Will the UDCLT transfer (including by providing remote access) personal information to third-party service providers located outside of the country in which the UDCLT collected the personal information?** | No | |
| **If yes, in which countries?** (check all that apply) | ☐ | EEA countries |
| | ☐ | Countries deemed adequate by the EU (Andorra, Argentina, Canada (commercial organizations only), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay) |
| | ☐ | United States |
| | ☐ | Other (please specify): _____ |

| 6. Technical and Organisational Measures[4] | | |
|---|---|---|
| **What technical and organisational measures will be used to protect the personal information?**[5] (check all that apply) | **Physical Security Controls** | |
| | ☐ | Identification card for all members of staff |
| | ☐ | Manned reception area in all buildings |
| | ☐ | Visitor access procedure |
| | ☐ | Locked entry gates at all external doors |
| | ☐ | Data center access limited to authorised personnel |
| | ☐ | Entry security systems 24x7 (such as smart card reader, code locks) |
| | ☐ | Intrusion detection alarm |
| | ☐ | Clear-desk policy |
| | ☐ | Locks for filing cabinets containing sensitive data |
| | ☐ | Monitoring devices (such as camera) |
| | **Access Security Controls** | |
| | ☐ | Access control system (user ID and strong password). Two factor authentication for remote access |
| | ☐ | Screen logs that activate after period of inactivity |
| | ☐ | Encryption of data on personal computers, portable devices, or removable media |
| | ☐ | Encryption of data transmitted via unsecure networks |
| | ☐ | Firewalls |

[4] GDPR does not prescribe specific security measures. This is an illustrative list. We can add any other security measures which the UDCLT takes.

[5] Please note that this is a comprehensive list of technical and organizational measures. It is not necessarily expected that the UDCLT employs all of these measures, but given that the UDCLT processes special categories of data, particularly in relation to employees and volunteers, it would be best practice to employ as many of the measures as possible.

| | | |
|---|---|---|
| | ☐ | URL filtering |
| | ❒ | Penetration testing |
| | ☐ | Automated vulnerability scans |
| | ❒ | Documented security incident response plan |
| | **Authorisation Process** | |
| | ❒ | Documented request process for the introduction of new hardware and software |
| | ☐ | Documented authorisation process to grant only the minimum access required for each member of staff to perform his/her work duties |
| | ☒ | Regular controls of authorisations granted and change process to reflect termination of employment, contract, agreement, or change of roles |
| | ☒ | Privileged access limited to essential administration personnel |
| | ☐ | Authentication process (user ID and strong password) |
| | ☐ | Audit logs for servers, applications and network devices |
| | ☐ | Secured interfaces |
| | ☐ | Disk management |
| | ❒ | Encryption of data on personal computers, portable devices, or removable media |
| | ☐ | Encryption of data transmitted via unsecure networks |
| | **Transmission Control** | |
| | ☐ | Encryption of data transmitted via unsecure networks |
| | ☐ | Encryption of storage media in transport |
| | ☐ | Personal firewalls |
| | ☐ | Electronic signatures |
| | ☐ | Fax protocols |
| | **Input Control** | |
| | ☐ | Access logs and analysis to ensure that it is possible to verify what personal data were entered into processing systems, modified, or removed, at what time, and by whom |
| | ☐ | Authentication process (user ID and strong password). Two factor authentication for remote access |
| | ☐ | Documented data retention schedule |
| | ☐ | Documented incident response plan |
| | **Availability Control** | |
| | ☐ | Daily automated back-up |
| | ☐ | Redundant power feeds |
| | ☐ | Temperature and humidity controls and monitoring |
| | ☐ | Encryption of data transmitted via unsecure networks |

| | | |
|---|---|---|
| | ☐ | Antivirus/firewall |
| | ☐ | Business continuity plan |
| | **Internal Policies and Training** | |
| | ☒ | Director/Trustee briefing on information security |
| | ☒ | Written security policies and procedures |
| | | |

**Changes to this inventory record**

The UDCLT reserves the right to amend this Article 30 UK GDPR Inventory from time to time in accordance with the UK GDPR and other applicable data protection requirements.

Effective Date: 1 March 2022

Last modified: 1 March 2022