POLICY DOCUMENT

Data Protection Policy

Document no:	9.0.2021
Version:	6.0
Responsible:	General Counsel (“GC”)
Approved by Board of Directors on:	1st December 2021

DATA PROTECTION POLICY

Table of Contents

1. BACKGROUND AND PURPOSE

Catena Media plc (the "**Company**") and its subsidiaries (jointly referred to as the "**Group**") need to gather and use certain information about individuals. This can include customers, suppliers, business contacts, consultants, freelancers, employees, and other people with whom the Group has a relationship with or may need to contact.

This Data Protection Policy (the "Policy") for the Group has been developed with the aim of ensuring that the Group:

- Complies with data protection laws and follows good practice
- Creates a framework for cross-border data transmissions within the Group
- Protects the data protection rights and freedom of individuals
- Shows transparency about collection and processing of personal data
- Prevents and manages risks of a data breach
- Is a trustworthy business partner and an attractive employer.

This Policy is applicable whenever processing of personal data takes place within the Group.

2. AUDIENCE

This Policy applies to all directors, employees (including interns, apprentices, trainees), independent contractors, Founders on earn-out and other similarly contracted workers (collectively known as "Relevant Persons").

3. SCOPE

This Policy includes accepted data protection principles and supplements the applicable data protection laws and regulations in each relevant country where a Group company carries out business. The relevant national law will take precedence in the event that it conflicts with this Policy, or it has stricter requirements.

These rules apply regardless of whether personal data is stored electronically, on paper or on other materials.

In addition to this Policy, the Group has developed, and will continue to develop when needed, supporting documents (e.g. procedures and instructions) addressing various privacy and data protection matters.

4. DEFINITIONS

"applicable laws" means all legislation and regulations (including those issued by competent supervisory authorities) protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data that from time to time apply to the Group, including Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the

processing of personal data and on the free movement of such data (General Data Protection Regulation, GDPR).

"Catena" means the relevant Group company.

“data breach” is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

“data controller” is the legally independent company of the Group who decides the purpose and use of personal data and whose business activity undertakes the relevant processing measure.

“EEA” is the European Economic Area (EEA), including the EU member states, Norway, Iceland and Liechtenstein.

"personal data" means any information relating to an identified or identifiable natural person, for example names of individuals, contact details, email, phone number and any other information relating to an individual.

“processing’ means any operation or action performed on personal data, for example collection, recording, storage, adaptation, consultation, use, disclosure, erasure, or destruction.

“profiling” means automated processing of personal data to “map” personal aspects, such as analysing or predicting health, personal preferences, interests, behaviour, location, or movements.

“registers” means structured registers of systems and contexts regarding personal data.

“third country” is a country outside the EEA, except countries having a data protection level that is considered sufficient by the EU Commission.

5. PRINCIPLES FOR PROCESSING OF PERSONAL DATA

Data protection is underpinned by a number of important principles that the Group should adhere to.

5.1 Lawfulness, fairness, and transparency

Personal data must be processed *fairly and lawfully* (meaning that there must exist a legal basis for the processing and an individual´s rights and freedoms must be protected).

A *fair processing notice* (for example a website privacy policy, and if applicable, cookie policy) regarding the processing of personal data must be provided to individuals whose personal data is being collected and processed (for example our websites and applications end-users, our employees and our customers) and must be presented **before** their personal data is being collected and processed. It shall, among other things, clearly set out who the data controller is, the purposes of processing, data subject rights and third parties to whom the personal data may be transferred. Relevant Persons must consult the Guidance on how to maintain our Privacy and Cookies Policies for further assistance in this regard.

Catena shall maintain a register of its processing of personal data in order to fulfil lawfulness, fairness and transparency.

5.2 Purpose limitation and data minimisation

Personal data must be collected only for *specific, explicitly stated, and lawful purposes*.

Personal data must be *adequate* and relevant and not collected in excess of what is *necessary and proportional* in light of the purposes of the processing (data minimisation). Before any new processing of personal data occurs, Catena must determine whether and to what extent the processing of personal data is necessary in order to achieve the purpose for which it is undertaken. If the new processing involves personal data already collected by Catena (but for other initial purposes) Catena must also look that the new processing is compatible with the purpose for which data was originally collected or if not, obtain consent or make sure it satisfies another legal basis (see section 7 below). Relevant Persons shall consult with the Legal and Compliance team in this regard. All purposes must be documented in a privacy policy as per Section 5.1 above.

Where the purpose allows it and where the expense involved is in proportion with the purpose being pursued, anonymized or statistical data use is advised. Personal data may not be collected in advance and stored for potential future purposes unless required or permitted by applicable laws.

Privacy by design and *privacy by default* shall be an integrated part of data processing at the Group. This means that any system, software, or technology shall be developed or used in a way that respects the principles of data processing in this section 5. More info on privacy by design and by default is to be found in the Group Privacy by Design and Privacy by Default Procedure.

5.3 Accuracy

Personal data must be accurate and where necessary kept up to date.

Relevant Persons will take reasonable and suitable steps to ensure, on a regular basis, that personal data they deal with is kept up to date (for example by asking data subjects whether there have been any changes, by implementing technical controls/features on the websites/applications etc).

Inaccurate or incomplete personal data will either be deleted, corrected, supplemented, or updated.

For further information, please consult the Data Accuracy Procedure.

5.4 Storage limitation

Personal data must not be held longer than necessary in light of the purposes of the processing (c.f. Section 5.2 above). Personal data shall be deleted or made anonymous when there no longer is a legal basis or legal obligation to keep it (including a need for the Group to establish or defend its legal rights).

Relevant Persons will ensure to either securely delete or make anonymous personal data where no longer required.

5.5 Integrity and confidentiality

Personal data is subject to confidentiality. Any unauthorized collection, processing, or use of such data by Relevant Persons is prohibited. Any data processing undertaken by a Relevant Person that he/she has not been authorized to carry out as part of his/her legitimate duties is unauthorized. The "need to know" principle applies. Relevant Persons may have access to personal information only as is appropriate for the type and scope of the job duties or task in question. This requires a careful breakdown and separation, as well as implementation, of roles and responsibilities. Relevant Persons are forbidden to use personal data for private purposes, to disclose it to unauthorized persons, or to make it available in any other way. Managers must inform Relevant Persons at the start of the relationship about the obligation to protect data secrecy. This obligation shall remain in force even after a Relevant Persons engagement has ended.

Personal data must be protected by appropriate organizational and technical measures, in line with Catena IT and Information Security Policies and taking into account industry standards, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of individuals to prevent unauthorized access, illegal processing or distribution, as well as accidental loss, modification or destruction. The responsible Relevant Person shall consult with the Security, Tech-Ops and the Legal and Compliance teams in this regard.

Measures that Catena Media can implement to safeguard personal data from unauthorized access and unlawful processing or disclosure, can include, but not limited to:

- the pseudonymization (where appropriate) and encryption (where appropriate) of personal data;
- measures that prevent transfer of personal data to any unauthorised person/entity, including secure communication by way of encryption of personal data in transit;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, e.g., by ensuring that personal data is backed up on a regular basis;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;
- appropriate back-up and disaster recovery solutions shall be in place. Regular testing of systems and protective measures shall be made;
- ensure that access to personal data shall be limited to personnel who need access for their work, and appropriate security should be in place to avoid unauthorised sharing of information; and
- conduct a privacy impact assessment before the use of a product, service, tool or provider that involves processing of personal data which may potentially present a high risk for rights and freedoms of individuals a data protection impact assessments

shall be made. Consult the Group's Data Protection Impact Assessment Procedure for more information in this regard.

These measures shall be evaluated at regular intervals in line with developments and organizational changes

6. DATA SUBJECT RIGHTS

Individuals have certain rights regarding their personal data and any requests for the exercise of such rights shall be dealt with in a timely and transparent manner (normally within one month). If Relevant Persons receive such a request, they will forward it as soon as possible to privacy@catenamedia.com

All data subject requests shall be handled in accordance with the Group's Data Subject Rights Procedure and recorded in a register to allow the Group to submit any information requested by a supervisory authority as well as establish or defend legal rights.

Data subject rights comprise:

◊ *Right of transparent communication and information*

Individuals may request information whether Catena holds personal data about him or her, where collected, for what purpose and if transmitted to a third party.

◊ *Right of access*

Individuals have a right to obtain information/copy about personal data processed regarding him or her.

◊ *Right to rectification*

Personal data shall be accurate, and individuals may request changes.

◊ *Right to erasure ('right to be forgotten')*

If no legal basis exists for keeping a set of personal data, for example a withdrawn consent, personal data must be deleted unless Catena has an overriding legal basis to keep.

◊ *Right to restriction of processing*

If an individual contests Catena´s processing of personal data, it shall be made unavailable or kept separate depending on the circumstances.

◊ *Right to data portability*

If processing is based on the individual´s consent or by contract, personal data of that individual shall be provided in structured, commonly used and machine-readable format.

◊ *Right to object*

An individual can object to Catena´s processing of personal data and that must be respected unless Catena can demonstrate that there is a compelling legitimate interest. If the objection pertains to direct marketing and thereto related profiling (see definition in section 4), Catena shall immediately stop processing such personal data.

◊ *Right to not be subject to automated decision-making (including profiling)*

If automated decisions are taken by Catena and produces legal effects regarding an individual, suitable safeguards shall be in place to allow the individual to be fully informed, respond and request the intervention of an employee at Catena Media.

7. LEGAL BASIS

Collecting, processing, and using personal data is permitted only under the following legal bases. One of these legal bases is also required if the purpose of collecting, processing, and using the personal data is to be changed from the original purpose.

Therefore, all personal data processed by the Group must be done on one of the following lawful bases:

- *Consent*: the individual has given consent for one or more specific purposes. The individual shall be given clear, concise, and specific information about the processing of personal data before giving consent. The granting of consent shall be documented. Further, the individual shall have a right to revoke the consent at any time and appropriate functions and systems shall be in place for that purpose. Relevant Persons shall consult Catena's Consent Guidelines for further information in this regard.
- *Contract*: as necessary for the performance of a contract with the individual.
- *Legal obligation*: necessary for compliance with a legal obligation.
- *Vital interest* (of individuals): necessary in order to protect the vital interests (for example medical urgency).
- *Legitimate interest*: necessary for the purposes of the legitimate interests and such interests are not overridden by the interests or fundamental rights and freedoms of the individual.

In relation to any processing of personal data, Catena shall note the legal basis in the register used for the mapping of personal data processing activities within the Group. Relevant Persons shall consult with the Legal and Compliance team in this regard. The legal basis must

be as well documented in a fair processing notice (for example website privacy policy, and if applicable, cookie policy) as per Section 5.1 above.

8. UNSTRUCTURED PERSONAL DATA

Personal data at Catena may not always come or be handled in a structured manner. Unstructured personal data is a set of raw and disorganized data that cannot be stored in predefined relational data structures. Examples of this type of data include email or slack messages, text files like PDF files or spreadsheets, user-generated content via forums or customer support.

Unstructured personal data is obviously more of a challenge to deal with - the amount of such data combined with its unstructured nature makes it considerably more difficult to gain an overview and manage the data being processed. However, Catena must still ensure privacy principles are adhered to here as well.

Keeping unstructured personal data limited is important and every Relevant Person needs to work in a way that takes this into consideration. In this regards, best practices include but are not limited to:

- Inboxes should not be used as archives for the long-term storage of old email – important business information shall be saved in appropriate locations/folders. Each Relevant Person is responsible for managing emails (including disposal when no longer needed).
- When sending an email, careful consideration should be given as to whether personal data needs to be used. This applies not only to what is written in free text but also to any email attachments. Avoid sending attachments containing a lot of personal data via email where documents may be shared in other ways, such as via a link or shared file system. Do not enter personal data into the subject line of the email.
- Avoid using sensitive personal data in emails entirely. For example, if you wish to state that someone is absent due to illness, it is enough to write that the person in question is ‘absent’, while omitting the detail that the person is actually ill.
- Identify files and documents containing personal data and store/name/assign them appropriately and securely.
- Avoid storing personal data on desktops, laptops, tablets, or smartphones.
- Avoid entering personal data when filling in free text fields.
- Avoid saving private documents, files, pictures or video or audio recordings in IT systems or equipment provided by Catena.
- Make an assessment in each case as to whether you need to use personal data in a document. If this is not required, you should avoid doing so.

9. DATA TRANSFERS

If a Catena Media company a) is established in the EEEA or b) processes personal data about people within the EEA, such personal data **must not**, as a general rule, be transferred to a third country (i.e. outside the EEA),unless it ensures an adequate level of protection or appropriate

safeguards are in place. Here (https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en) the European Commission publishes the list of countries outside the EEA which the European Commission deems offer an adequate level of data protection.

Further, in all cases, transmission of personal data to third parties outside the Group must be made based on a legal basis (see Section 7) and upon the conclusion of a data processing agreement (DPA). A DPA must be concluded in writing with a third party (processor) who processes personal data on Catena´s behalf. The processor must be chosen based on demonstrated ability to comply with this Policy and its undertaking to process personal data on Catena´s instructions only and in accordance with applicable law. When contracting a new third party who processes personal data on Catena´s behalf, attention shall be given to the rules and procedures found in Group's Processor Management Procedure.

Transfer of personal data within the Group shall be made in accordance with an Intra-group data transfer agreement.

10. PERSONAL DATA BREACHES

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity, or availability of personal data.

Catena Media must take appropriate measures to detect and, if necessary, report personal data breaches. If reporting to authorities is needed, Catena must do so within 72 hours of becoming aware of the reportable breach.

In the event of a data breach, Catena shall immediately assess and take measures to eliminate the risk to people's rights and freedoms and, if appropriate, report the data breach to relevant supervisory authority and individuals concerned. If not addressed in an appropriate and timely manner, a personal data breach or security incident has the potential to result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative non-compliance and/or financial penalties for Catena. All data breaches shall be recorded in a register (also when a data breach is not reported to the supervisory authority/individuals concerned) and handled in accordance with the Group's Personal Data Breach Procedure.

Responsibility for reporting as soon as possible a suspected breach lies with the Relevant Person who discovered the breach or security incident.

11. DATA PROTECTION RISKS

This Policy helps to protect the Catena Group from data security risks, including:

- *Breaches of confidentiality***.** For instance, information being given out inappropriately or unlawfully.

- *Failing to show transparency***.** For instance, the Group must be transparent about the processing of personal data carried out in order to ensure that individuals are aware of the processing of personal data relating to them.
- *Reputational damage.* For instance, the Group could suffer reputational damage if an unauthorized person or organisation gained access to personal data.
- *Administrative fines, penalty, or damages***.** As decided by a supervisory authority or a court – maximum fine the higher of 20 000 000 euros or 4 percent of total worldwide annual turnover of the Group.

12. ROLES AND RESPONSIBILITIES

The Board of Directors is ultimately responsible for ensuring that the Group meets its legal obligations according to applicable laws.

Each company of the Group and each individual Relevant Person is responsible for compliance with this Policy and the national data protection laws applicable to it.

The GC is responsible for:

- Keeping the board updated about data protection responsibilities, risks, and issues.
- Reviewing all data protection procedures and policies, at regular intervals or as decided in a policy or procedure.
- Arranging data protection training and giving advice to staff, interns, volunteers, consultants, and other people working on behalf of the Group and covered by this Policy.
- Dealing with data subject rights requests (for example individuals´ right to get information about personal data that Catena holds about them).
- Approving any contractual arrangement with any third-party services that Catena is considering using to process personal data on its behalf (for instance, cloud computing services).

The CTO is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services Catena is considering using process personal data on behalf of the Group (for instance, cloud computing services).
- Arranging data protection security and integrity training and giving advice to the Relevant Persons.

All Relevant Persons with managerial responsibilities are responsible for:

- Informing the GC of any data protection queries from partners, third parties, customers, or media outlets.
- Working with the GC to ensure that the Group's products, marketing initiatives and data, sales data, product data and financial data abide by data protection principles.

All Relevant Persons have a responsibility for ensuring that personal data is collected, stored and handled appropriately and lawfully and in accordance with this Policy and the Group's other privacy procedures, guidelines or instructions, as applicable from time to time.

13. EXCEPTIONS

There are no exceptions to this Policy. Any need for exceptions to this Policy must be clearly defined and documented. All exceptions shall be approved by the Board of Directors.

14. REVIEWS AND UPDATES

The Data Protection Policy shall be reviewed, updated, and adopted when deemed necessary or appropriate, however, no less than annually.

The Data Protection Policy shall be reviewed and updated by the General Counsel and adopted by the Board of Directors.

15. REFERENCES TO ASSOCIATED DOCUMENTS AND LINKS

- IT and Information Security Policies
- Processor Management Procedure
- Data Subject Rights Procedure
- Data Protection Impact Assessment Procedure
- Personal Data Breach Procedure
- Guidance on how to maintain our Privacy and Cookies Policies
- Privacy by Design and Privacy by Default Procedure
- Data Accuracy Procedure