LEXACOM

Data Protection Impact Assessment

Chris Bohin

Version 1.3, 15/04/2025

Table of contents

Introduction

In the words of the Article 29 Working Party (now the European Data Protection Board), a Data Protection Impact Assessment (DPIA) is a process for building and demonstrating compliance. It is carried out to help identify and address data protection, privacy, and other related risks in projects (such as new systems/technology or processes) that are present within the design, development and implementation of the system or process (or where there are significant changes to an existing system or process).

Scope

DPIAs are required for processing activities that are likely to result in high-risk to individuals. This would mean that new and existing processes, projects and technologies that potentially pose a high-risk to individuals would need a DPIA in order to assess the risk and introduce measures to reduce the risk. If the DPIA identifies a high risk which cannot be mitigated, the Information Commissioners Office (ICO) must be contacted.

Processing that is likely to result in a high risk includes (but is not limited to):

- Systematic and extensive processing activities which are based on automated processing, including profiling and where decisions that have legal effects (or similarly significant effects) on individuals.
- Large scale processing of special[1] categories of data or personal data relating to criminal convictions or offences. Large scale systematic monitoring e.g., monitoring of public areas (CCTV).
- If unsure about whether a DPIA is required, refer to the DP02 DPIA Screening Questionnaire, to identify if the processing activity poses a high risk to the rights and freedoms of individuals.

Effects of non-compliance

Failure to carry out a DPIA when one is required, carrying it out in an incorrect way and/or failing to consult the ICO where required can result in a fine.

[1] *Special categories of data refer to personal data revealing racial or ethnic origin, political opinion, religious or philosophical beliefs or trade union membership, the processing of genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health or data concerning an individual's sex life or sexual orientation.*

Data Protection Impact Assessment

Background/project description

Project purpose	This assessment has been generated for the purpose of providing Lexacom customers with an overview of data processing within their application. The DPIA shall be considered as complementary to, or part of, a wider risk management process Lexacom must implement and perform. Indeed, although it is called an "assessment", the DPIA goes beyond the simple analysis of data protection risks, by describing adopted or envisaged safeguards and control measures in proportion to the risks identified, thereby being based on a risk management procedure rather than a mere risk assessment.
Concerns with project	That compliance requirements are satisfied, and data is protected as part of the customer's project deliverables.
Reason for DPIA	A DP02 DPIA Screening Questionnaire has been completed and identified that, due to the processing of special category data, a DPIA is required. There exist a number of important benefits when performing a DPIA. The following benefits are identified when using this DPIA: • Preventing costly adjustments in processes or system redesign by mitigating privacy and data protection risks. • Prevention of discontinuation of a project by early understanding of the major risks. • Reducing the impact of law enforcement and oversight involvement. • Improving the quality of personal data (minimisation, accuracy). • Improving service and operation processes. • Improving decision-making regarding data protection. • Raising privacy awareness within the organisation. • Improving the feasibility of a project. • Strengthening confidence of consumers, employees, or affected individuals in the way which personal data are processed, and privacy is respected. • Improving communication about privacy and the protection of personal data.

Processing description

Information flow

What is the source of the personal data? **How will you collect the personal data (from the individual directly, a third party, from records within your organisation etc)?**	The source of the data is primarily audio recordings of consultations and other dictations created by end users. These may include Personally Identifiable Information if the end user has chosen to include it in their dictations. This can also be documents which are attached to jobs within the application. Information required for the purpose of creating individual accounts within the application will be provided by the users or their employers.
What do you intend to do with the personal data? How will you use it? Where will it be stored?	Dictations provided by users will be converted into text and returned to the end user. Dictation data and user details are stored in a database within Lexacom's Azure cloud infrastructure. All data is restricted and isolated to each customer.
Who will have access to the personal data (internally and externally)?	Where data is accessed by Lexacom staff this is classed as internal access, it is controlled in line with Lexacom's ISO 27001 commitments via role-based access and is triggered only upon a customer request for access or support. End users will have access to their own information and dictations. End user organisations are responsible for managing and controlling access to data within their teams. There is no external access to any data.
Will you share the personal data with anyone outside the organisation?	No personal data is shared outside of Lexacom.
Will the personal data be transferred to another country? If yes, where?	No. All data remains in Azure UK South (London) or UK West (Cardiff) regions.
How long will the personal data be retained for?	By default, customer data is kept for 90 days before being permanently deleted. Customers are able to request a longer or shorter retention period if they require this. Tracking data is not deleted but this does not contain PII.
How will the personal data be disposed of?	All job media is deleted from the database and the entry will be marked as 'Deleted by time expiration'.

Nature of the processing

Scope of processing	The customer determines and controls, at its sole discretion, what information is uploaded onto the Lexacom platform. The customer determines and controls what information (and, in particular, the specific categories of data which the Personal Data transferred concerns) is processed by Lexacom in providing the services to the customer. The data processed within the Lexacom application may therefore contain personal details if the user has chosen to include this information within their dictation.
Context of the processing	A direct relationship does not exist between Lexacom and the data subjects.
Purpose of the processing	Lexacom is a platform offering workflow management, speech recognition, ambient AI, and digital dictation for the purposes of speech to be transcribed into text. The processing takes places for as long as the customer has a valid licence and maintains an ongoing agreement with Lexacom. Customers are responsible for submitting their data to the platform for processing. The intended effect on individuals is low, as the relationship with the data subject is maintained by industry professionals and is provided in line with their processes and code of conduct.
Legal basis for the processing	Lexacom will process personal data under Article 6 (1) (b) of the GDPR: processing is necessary for the performance of a contract to which the data subject is party. Processing under this lawful basis will include: (non-exhaustive for illustrative purposes) • Establishing access to the platform, software, or service under an agreement/ licence. • Onboarding, installing, and provision of user access to the platform, software, or service. • User support and guidance including technical issues. Lexacom will process personal data under Article 6 (1) (f) of the GDPR: processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Processing under this lawful basis will include: (non-exhaustive for illustrative purposes) • Troubleshooting (preventing, detecting, and repairing problems). • Ongoing improvement (installing the latest updates and making improvements).

Consultation process

Consultations	The DPIA team requires strong understanding of the Lexacom service itself, knowledge of data protection, privacy and cyber security and expertise in the performance of risk assessments. Because of the diversity of expertise and interests involved, it is common to conduct the DPIA with a small and multidisciplinary team where the following expertise is combined: • Risk assessment. • IT architecture and system engineering. • Information security. • Privacy and data protection. • Clinical safety. • Organisational design. • Project management.
Internal consultation	**Senior Management Team:** Dr Andrew Whiteley – Managing Director Gareth Murton – Finance Director Simon Brady – Head of Sales Chris Bohin – IT Manager **Development Team:** David Strachan – Lead Developer **Clinical Safety Officer:** Dr Simon Bentley **Data Protection Officer:** Chris Bohin **ISO Management System:** Senior Management Team
External consultation	**Data Privacy Consultants:** The DPO Centre Ltd. **ISO Auditors:** British Assessment Bureau **Users:** Lexacom customers and industry specialists
Individuals (data subjects)	Lexacom do not maintain a relationship with the customer's data subjects.

Assessment of necessity and proportionality

Compliance and proportionality measures in place	Lexacom continually work towards and maintain standards which ensure controls are in place to protect customer data. Lexacom is a trading name of Aprobrium Ltd, a limited company registered in England and Wales. Company Number 03835983. Information Commissioner's Office Registration Name: APROBRIUM LIMITED Registration Number: Z2646347 Lexacom is committed to protecting the security of personal information and use a variety of security technologies and procedures to help protect information from unauthorised access, use, or disclosure. To this end, Lexacom maintain the following accreditations. **Lexacom Accreditations** • Cyber Essentials Plus • ISO 9001 – Quality Management Services • ISO 27001 – Information Security • DCB0086: DSP Toolkit (Organization ID 8J566, be found on via the organisation search on https://www.dsptoolkit.nhs.uk. **Microsoft Regional/Country Compliance** • UK Cyber Essentials Plus, G-Cloud, PASF, Standard Contractual Clauses • IRE EN 301 549, ENISA IAF, Standard Contractual Clauses, GDPR **Microsoft Industry Compliance** • UK DPP, FACT, FCA/PRA, CDSA, GxP, PCI DSS, TruSight • IRE EBA, CDSA, GxP, PCI DSS, Shared Assessments, TruSight **Microsoft Azure** • ISO27018 – Code of practice for protection of personally identifiable information (PII) in public clouds https://docs.microsoft.com/en-us/azure/compliance/offerings/offering-iso-27018
Necessity	Processing of data within Lexacom is a necessary function, it serves the purpose of transferring speech to text. Feedback submitted is only used to improve the audio engine. Lexacom provides both desktop and mobile applications, enabling users to process data from any location. Lexacom's products have been created with the sole purpose of increasing efficiency in the workplace by reducing the burden of administrative tasks.
Proportionality	Data is processed primarily for the purpose of servicing the customer and supporting their workflow requirements, it is not monitored or reviewed at rest. The data may be accessed

	by the customer for their own audit records, or via Lexacom service teams if the customer requests support. Where processing is temporary, it is actioned via Microsoft Azure servers and automatically deleted once the audio has been transcribed. Data is processed primarily for the purpose of servicing the customer and supporting their workflow requirements, it is not monitored or reviewed at rest. Lexacom employs least privilege access mechanisms to control access to customer data (including any personal data therein). Role-based access controls are employed to ensure that access to personal data required for service operations is for an appropriate purpose and approved with management oversight. For example, the Admin Tracking feature gives the customer an overview of all current or historic dictations within their Lexacom application, this is restricted by password protected Lexacom Administrator access. If the customer requires further assistance with a dictation within Lexacom they can contact the Lexacom Helpdesk who may remotely access their PC, or they may raise a query on their database to view the information held therein. If the customer receives a request for access from their data subject, Lexacom as the processor can provide support using the audit functions or database queries, but only when requested. It is considered that the data processed is within the limits of what is needed for Lexacom to fulfil its service objective, and that the risks to fundamental rights are proportionate to the benefits of the processing activities.
Subject Rights	Lexacom in its role as a processor of personal data will make available to its customers, the ability to fulfil data subject requests to exercise their rights under the GDPR. If Lexacom receives a request from Customer's data subject to exercise one or more rights under the GDPR in connection with the platform or services for which Lexacom is a data Processor, Lexacom will redirect the data subject to make its request directly to Customer (the Controller). In all cases where possible Lexacom will support requests by the customer to assist with Customer's response to such a data subject request including rights of access, correction, restriction, objection, erasure, or data portability, as applicable.

Identify the privacy and related risk

Risks have been identified and assessed in line with the risk-based approach defined in Lexacom's ISO Management System – M001.

The Risk Score (RS) is calculated by applying and multiplying likelihood (L) and severity (S) of the risk occurring on a scale from 1-3. The confidentiality, availability and integrity of information should be a consideration.

Score	Liklihood	Severity	Risk Score
1	Possible	Minimal	1-3
2	Uncommon	Moderate	4-6
3	Probable	Significant	7-9

Risk mitigation will be assessed to identify how risks can be avoided or tolerated. The Risk Score is divided by the mitigation score, also on a scale from 1-3, to generate a Residual Risk score.

Score	Mitigation	Residual Risk
1	Accepted	7-9
2	Reduced	4-6
3	Removed	1-3

Data protection risk assessment

Risk	L	S	RS	Privacy & Compliance Impact	Mitigation Measures	M	RR
Lexacom data breach	1	3	3	A breach of Lexacom's systems could expose personal data, violating GDPR Articles 5(1)(f) (integrity & confidentiality) and 32 (security of processing).	Lexacom maintains an ISO 27001 certified Information Security Management System, subject to regular external audits, ensuring compliance with international security standards, including Cyber Essentials Plus and NHS DCB0129. Lexacom enforce strict access controls, encryption, and internal security policies, complemented by regular penetration testing and security audits. Lexacom is also compliant with UK Government G-Cloud security requirements.	2	1.5
Azure data breach	1	3	3	Lexacom relies on Azure cloud infrastructure, meaning a breach at Azure could impact hosted patient data, violating GDPR Article 5(1)(f) (integrity & confidentiality).	Microsoft Azure is certified to ISO 27001, Cyber Essentials Plus, and NHS DCB0086. Lexacom enforces strict access controls and applies encryption at rest and in transit, ensuring that only authorised Lexacom users can access stored data. Microsoft are also compliant with UK Government G-Cloud security requirements.	2	1.5
AI data breach	2	3	6	AI processing occurs within Azure, if AI processing is compromised, patient data could be exposed, violating GDPR Article 5(1)(f) (integrity & confidentiality).	Current versions of Lexacom do not use 3rd party AI providers. AI processing is carried out in the UK, ensuring compliance with UK data protection laws. Customers concerned about AI risks can disable AI powered features.	3	2
Unauthorised access	1	3	3	Unauthorised data access could result in a breach of GDPR Articles 5(1)(f) (Integrity & Confidentiality) and 32 (Security of Processing), leading to potential regulatory action.	Role-based access control (RBAC) ensures only authorised users can access specific data. Audit logs track all actions for accountability.	2	1.5
Incorrect user access	1	2	2	Assigning incorrect access permissions could expose personal data to unauthorised individuals, violating GDPR Articles 5(1)(f) (Integrity & Confidentiality) and 25 (Data Protection by Design & Default).	User accounts are controlled by the customer. Administrators appointed by the customer can revoke access immediately. No access to data is granted without login credentials.	2	1
Device compromise	2	3	6	A lost or stolen device containing unprotected patient data could violate GDPR Articles 5(1)(f) (Integrity & Confidentiality) and 32 (Security of	Lexacom mobile app includes PIN protection and remote disable functionality. Customers are advised to enable device-level security controls, such as login authentication and device encryption.	3	2

				Processing) by failing to secure personal data against loss or theft.			
Loss of internet access at customer site	2	2	4	Could disrupt workflows but does not directly impact privacy unless data cannot be accessed when needed for care.	Lexacom provides an offline mode with basic functionality, including offline speech recognition. Dictated audio is securely stored locally and uploaded once internet access is restored.	2	2
Speech recognition misinterpretation	2	3	6	Could lead to inaccurate patient data being stored, violating GDPR Article 5(1)(d) (Accuracy), which requires that personal data be accurate.	Lexacom provides training and best practice guides to improve accuracy. Continuous model updates refine performance. Users are advised to review all output before use.	3	2
Comprehension Engine® misinterpretation	2	3	6	Could lead to inaccurate patient data being stored, violating GDPR Article 5(1)(d) (Accuracy), which requires that personal data be accurate.	Comprehension Engine® follows deterministic processing rules to ensure predictable transformations. Regular updates and user feedback improve accuracy. Users are advised to review all output before use.	3	2
Comprehension Engine® Medical Mode error or omission	2	2	4	Could lead to inaccurate or incomplete patient data being stored, violating GDPR Article 5(1)(d) (Accuracy), which requires that personal data be accurate.	Medical Mode follows NHS standard practice for abbreviations and clinical shorthand. Users can customise shorthand settings using text snippets. Users are advised to review all output before use.	3	2
Comprehension Engine® Patient Mode error or omission	2	3	6	Could lead to inaccurate or incomplete patient data being stored, violating GDPR Article 5(1)(d) (Accuracy), which requires that personal data be accurate. If there is an oversimplification, this could conflict with GDPR Article 12 (Transparent Communication), which requires that information be clear and understandable.	Patient Mode follows NHS guidelines on plain English for health communication and has undergone extensive independent testing, including public surveys. It is optional and can be disabled. When enabled, the original text remains visible alongside the simplified version (in brackets) to ensure transparency. Users are advised to review outputs before sharing with patients.	3	2
AI unintentional data retention or training on patient data	2	3	6	If AI systems are inadvertently configured to store data or use it for model training, patient data could be retained without consent, violating GDPR Article 5(1)(e) (storage limitation).	Current versions of Lexacom do not use 3rd party AI providers. AI processing is carried out in the UK, ensuring compliance with UK data protection laws. Customers concerned about AI risks can disable AI powered features.	3	2

Patient Shield partial or failed redaction	1	3	3	Patient Shield reduces risk by redacting most identifiable data, though some personal data may remain if redaction is incomplete. This could still lead to potential GDPR Article 5(1)(c) (data minimisation) and 5(1)(f) (security) concerns if unredacted data is processed further.	Patient Shield redacts names, dates, NHS numbers, phone numbers, email addresses, and addresses using natural language processing and deterministic methods. Customers can opt for local redaction on the user's device before any AI processing. Users are advised to review outputs manually to ensure full redaction.	3	1
Audit logging deficiencies	2	3	6	A lack of robust logging could make unauthorised access difficult to detect, breaching GDPR Article 5(1)(f) (integrity and confidentiality).	Lexacom maintains detailed, tamper-proof audit logs of all data access and modifications.	3	2
Lack of Multi-Factor Authentication (MFA)	2	3	6	Single-factor authentication increases the risk of data breaches, violating GDPR security principles.	Lexacom supports MFA for all user accounts. Customers are strongly advised to enforce MFA policies to reduce unauthorised access risks.	3	2
Software bug leading to unintended data exposure	2	3	6	If a software bug causes unintended data exposure, this could violate GDPR Articles 5(1)(f) (Integrity & Confidentiality) and 32 (Security of Processing) by failing to protect patient data.	Lexacom ensures rigorous quality assurance and penetration testing before deployment. Security patches are prioritised. Users are advised to report unexpected behaviour immediately.	3	2
Insecure third-party integrations	2	3	6	Poorly secured third-party integrations increase the risk of patient data breaches.	Third-party integrations must meet Lexacom security standards before approval. Customers are advised to perform security assessments on external systems.	3	2
Data retention & deletion compliance	2	3	6	Holding patient data beyond required retention periods could violate GDPR Article 5(1)(e) (storage limitation).	Lexacom ensures automated data retention policies with controlled deletion processes.	3	2
Accidental disclosure of patient data in support request	2	3	6	Could result in unauthorised processing or retention of patient data, potentially violating GDPR Article 5(1)(c) (data minimisation) and Article 6 (lawful basis for processing).	Lexacom support staff are trained in GDPR compliance and will immediately inform customers of any accidental disclosure discovered . Any received patient data is not stored and is permanently deleted per GDPR guidelines. Customers are advised to anonymise or redact data before sharing, and to close other applications or documents on their system before asking for help using screen sharing and remote access tools.	3	2

Accidental disclosure of patient data in product feedback	2	3	6	Could result in unauthorised processing or retention of patient data, potentially violating GDPR Article 5(1)(c) (data minimisation) and Article 6 (lawful basis for processing).	Customers are advised not to include patient-identifiable data when submitting feedback. Any received patient data is not stored and is deleted immediately in line with GDPR policies.	3	2

Identify sign-off and record DPIA outcomes

	Name/Position/Date	Notes
Mitigation measures approved by:	Lexacom Senior Management Team 03/03/2025	Refer to 4.2 Internal Consultation
Residual risks approved by:	Lexacom Senior Management Team 03/03/2025	No Medium or High residual risks before or after mediation.

Summary of DPO advice

The DPIA has been completed in consultation with the DPO ensuring individual rights have been considered throughout the project journey. Lexacom and the consultation team have assessed the possible effects to individuals and have applied suitable measures to manage and minimise any possible distress or harm.

Lexacom have established technical and organisational measures in place to handle and process data collected in compliance with the GDPR. Suitable procedures are in place to manage any complaints, withdrawal, and facilitation of data subject rights.

Lexacom remain entirely satisfied that this DPIA more than adequately describes the nature of processing envisaged, lawful basis, necessity, proportionality, controls, and mitigations in line with Article 35 of the UK GDPR.

	Name/Position/Date	Notes
DPO advice accepted or overruled by:	Lexacom Senior Management Team 03/03/2025	Accepted
This DPIA will be kept under review by:	DPO	Review to be undertaken annually to monitor for change
Date of next review:	03/03/2026	

Integrate the DPIA outcomes into the project plan

Who is responsible for integrating the DPIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved?

Action to be taken	Date for completion of actions	Responsibility for completion of action
Annual Review – monitor in 12 months for any change	March 2026	DPO

ICO notification

If you have decided to accept a high risk, either because it is not possible to mitigate or because the costs of mitigation are too high, you must consult the ICO before you go ahead with the processing. The submission should be sent to DPIAconsultation@ico.org.uk and include all the following elements:

- a description of the respective roles and responsibilities of any joint controllers or processors;
- the purposes and methods of the intended processing;
- the measures and safeguards taken to protect individuals;
- contact details of your DPO; and
- a copy of the DPIA

Date notification made to ICO	N/A – no High Risks identified