

Data Management and GDPR



At Lexplore Analytics our team is committed to protecting your school data.

We have standardised policies in place for the protection of all school data. These are regularly reviewed by our experienced team and ICO registration.

We do not store more information than is required for our assessment and all personal data is handled in separate encrypted databases which use traffic encryption and secure two-step authentication practices.

Lexplore



Data handling and GDPR

Even at the beginning, research stage of the Lexplore Analytics journey data protection was of top priority for Optolexia, the company which then became Lexplore Analytics. Developed following extensive research at the Karolinska Institute, which has selected the Nobel Laureates in Medicine and Physiology since 1901, our team are accustomed to working with strict data protection requirements. However, when GDPR came into effect under EU law in the Spring of 2018, we carried out several investigations with the help of both internal and external specialists in law and data security. Lexplore Analytics met and exceeded the secure data processing requirements which exist under The General Data Protection Regulation act (GDPR).

New GDPR demands

During the two years that Lexplore Analytics has existed in the UK, data processing regulations have changed dramatically, especially under the 2018 The Data Protection Act, which currently supplements and tailors GDPR policy within the UK.

To ensure that Lexplore analytics still meets the new requirements that exist under DPA and GDPR provisions, we have carried out a thorough investigation and a review of practices, using both the expertise of our internal experts as well as external data protection professionals.

Questions addressed in the enquiry

- 1. Are voice and eye movement recordings considered as biometric data under the new data protection regulation?*
- 2. Is reading attainment considered as health data under the new data protection regulation?*
- 3. Is the data that Lexplore Analytics processes special category data under the new data protection regulations, and if so, does Lexplore Analytics meet the requirements for extra protection?*

Conclusion of the enquiry

- 1. Compliance to article 9 of the Data Protection Regulation on Biometric Data is not required for the processing of data during the Lexplore assessment as eye movement and voice recordings are not used for identification purposes.*
- 2. AI analysis by Lexplore provides results on reading attainment. Reading attainment is not health data but educational data already used in schools*
- 3. Despite reading attainment not being health data, all personal data handled by Lexplore Analytics is extra protected and Lexplore meets these strict requirements.*

GDPR

The Data Protection Regulation Act 2018 (DPA 2018) controls how all personal information is used by organisations, businesses and the government in the UK. It acts as the UK's implementation of General Data Protection Regulation (GDPR) under European Union (EU) law. GDPR aims, among other things, to create "a uniform and equivalent level of protection for all personal data" (The Data Inspectorate). Before GDPR came into force, the UK's Data Protection Act 1998 enacted the provisions set out under the EU's Data Protection Directive 1995. Many organisations, therefore, already had strict and effective strategies in place to protect personal data, even before GDPR.

Your data protection rights

Data protection policy ensures the fair and proper use of information about people. As part of the UK's data protection regime, both DPA 2018 and GDPR protect your fundamental right to privacy. These regulations apply to all businesses, associations and organisations, as well as individuals who process personal data for non-private purposes. GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

More Information about your individual rights can be found by visiting the Information Commissioner's Office (ICO) Website - [HERE](#)

What is personal data?

Personal data is any information that relates to an identified or identifiable individual. This can be as simple as names, addresses and numbers, but even pictures and voice recordings are regarded as personal data, even if names are not mentioned. Personal data also includes other identifiers, like IP addresses or cookies.

Data Controllers and Processors

Controllers are the main decision makers when it comes to handling personal data. They have the highest compliance and responsibility to the principles of GDPR. Processors act on behalf of and under the instruction of Controllers. Processors do not have the same obligations as Controllers and do not have to pay a data protection fee. If two or more controllers jointly determine the purposes and means of the processing of the same personal data, they are joint controllers. However, they are not joint controllers if they are processing the same data for different purposes.

Lexplore Analytics processes data on behalf of the customer or school with responsibility for the personal data.



Biometric data for identification (Governed by article 9 of the GDPR)



Fingerprint



Eye recognition



Face Recognition



DNA

Biometric data with other purposes



Eye movements to
measure reading



Voice recording to
assess reading



School pictures



Recordings in
classrooms for teaching

Biometric personal data

The Data Protection Regulation defines Biometric data as “data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person.”

When you use fingerprint recognition and facial recognition to unlock your mobile, this is using biometric data. All biometric data is personal data, as it allows or confirms the identification of an individual. Biometric data is also special category data whenever it is processed “for the purpose of identifying a natural person”. Under DPA 2018 and GDPR, special category data merits extra, specific protection.

The use of this data could create result in significant risks to fundamental rights and freedoms. It is, therefore, to be handled and processed with greater care. This is part of the risk-based approach of the GDPR.

Are eye movement recordings special category data?

Eye movement recordings from the Lexplore assessment are used to determine reading attainment and analyse reading patterns. These are not used for identification. During the Lexplore assessment, the eye tracker simply monitors how a child’s eyes move across a text.

Iris Scanning for Identification

The iris of your eye is as unique as your fingerprint! The colour and shape varies for every individual and, therefore, a scan of the iris can be used to identify individuals. For the Lexplore Assessment, the eye and iris’ appearance does not influence the analysis of reading. Therefore, no such images, data or iris scanning technology is used.

Health data

Health data is defined as any “personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.” This also includes any information on health that comes from tests, information such as illness, disease risk or disability regardless of the source of this data.

In schools, this relates to any information relating to pupils’ health.

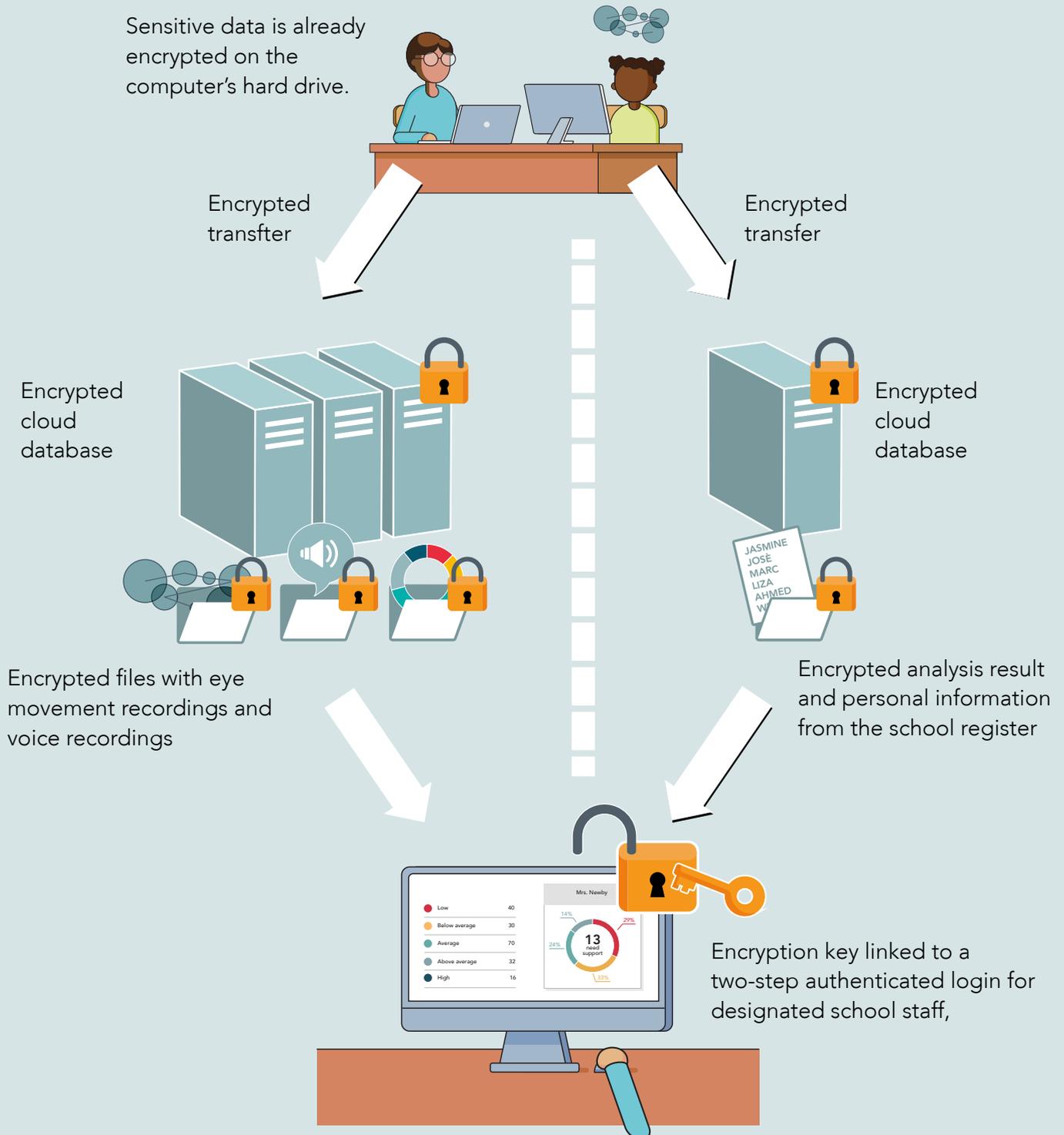
Lexplore Analytics does not process or handle health data. It is also not possible to offer a diagnosis of any illness or learning difference directly from the testing service.

Is it forbidden to manage personal data?

All businesses, companies and organisations, including schools handle personal data in some form. It is not in any way prohibited to handle personal data, the requirement is that you must have a valid reason for doing so and that you do it safely.

Encrypt and separate

A basic principle of Lexplore Analytic's data protection strategy is to separate and encrypt the information we collect as much as possible. Eye movement recordings and voice recordings from the assessment are stored in separate, encrypted databases for each organisation. These are stored without names or any identification numbers. This data is only combined within the Result's Portal using an encryption key. Your eligibility level and role within the portal will then determine which results you have access to within this Portal. This can only be accessed through a secure two-step authentication process.



Lexplore Analytics and Data Protection Regulation

As a new company, Lexplore Analytics have not had to make significant changes to existing systems and routines in relation to new data protection regulation. We have instead been able to use the regulation during the initial development of our IT systems and routines.

Privacy by design

Privacy by design means that Data Protection Regulation has acted as a guiding principle during the process of developing Lexplore Analytic's IT systems. At each step of the process, many considerations have been made to ensure personal data is protected. For example, no personal data is stored if not needed, any data that needs to be sent will be encrypted and results portal data can only be accessed through a secure two-step authentication process. Data protection regulation has, therefore, been met since the start of Lexplore.

What data does Lexplore handle?

At Lexplore Analytics we have standardised policies and procedures to ensure that the data we process as part of our assessment service is protected in accordance with Data Protection Regulation, Cyber Security Law and our registration with the ICO. To ensure these are kept up to date, our team, who have an inherent knowledge and are experienced in working within education and data protection, conduct regular policy reviews. Policies are also maintained through our ICO registration.

The Information Commissioner's Office (ICO) is the independent regulatory office in the UK. They are in charge of upholding information rights in the interest of the public. Under the Data Protection Act 2018, all organisations that process personal information must register with the ICO. The ICO then publish the names and addresses of the data controllers. They also include a description of the type of processing that each organisation performs.

Details of Lexplore's ICO registration can be found - [HERE](#)

For our assessment service we process personal data for:

1. Designated contact persons at the school.
2. Users of the Results Portal.
3. Pupils tested during the assessment service.

Designated Contact Persons

As the designated contact person at the school, we process the following information about you:

- Name
- System authorisation
- Telephone number
- Email address
- Details of your employer

Why do we process this data?

The processing of the above personal data is necessary to enable our subsidiaries and / or distributors to perform the agreement they have with the Customer.

In the event such data is not provided, the agreement with the Customer cannot be performed. Processing is undertaken based on the performance of that contract or our legitimate interests.

Your name and contact details are stored in our register of contact persons for the terms and duration of the contractual relationship with the Customer, or for such time as we otherwise require the information for any circumstance associated with the contractual relationship with the Customer.

In the event that your employment with the Customer terminates or you otherwise cease to be a contact person for the Customer, we will remove your data from our register.

Your data may occur in agreements and / or correspondence and documentation for the Customer. This personal data must be stored for commercial, business and legal reasons.

We may also store your personal data for an extended period of time if necessary to perform a legal obligation, which requires processing according to applicable law, or to enable us to establish, assert or defend legal claims.

Marketing

We and our subsidiaries also process your email address in order to distribute our marketing. In such a case, the marketing is directed at the Customer and based on the type of services that the Customer has previously purchased and which we believe to be relevant for you in the exercise of your profession.

The marketing is sent for up to five years after the Customer's most recent purchase. Newsletters and marketing emails are sent on the condition that no opposition has been expressed. You are entitled, at any time, to deregister from our newsletter and marketing emails. To do so, kindly contact us at hello@lexplore.com. or use the attached deregistration link in each newsletter/email.

Users of the Results Portal

As a user of the Results Portal, we process the following data about you:

- Name
- System authorisation
- Telephone number
- Email address
- Details of your employer

We also process data about your activity in the Results Portal, referred to as user data as follows:

- System authorisation
- Date of most recent login
- Performed administrative measures
- User log (time, city, IP address etc)
- Cookies

Why do we process this data?

The information is processed to enable you to use the Results Portal. Your name and your authority role are used to enable Customers to see which users are in the Portal. The details of your employer are used to allocate correct authorisation. Your email address is used as your unique login name and your telephone number is used solely to facilitate secure login using two-step authorisation.

Your role is associated with the specific organisation, school or class for which you use the Results Portal and decides which authorisation you possess.

Other data is processed to enable the Portal to function in the best manner. By processing such data we are able, among other things, to follow up if something goes wrong or if the Results Portal has in some way been misused.

How long do we store your data?

Your data is stored for the duration of the contractual relationship with the Customer and during the period in which we provide results via the Results Portal. In the event that your employment with the Customer terminates or you otherwise cease to be a user of the Results Portal, your data will be deleted/anonymised.

Marketing

We and our subsidiaries also process your email address in order to distribute our marketing. In such a case, the marketing is directed at the Customer and based on the type of services that the Customer has previously purchased and which we believe to be relevant for you in the exercise of your profession.

The marketing is sent for up to five years after the Customer's most recent purchase. Newsletters and / or marketing emails are sent on the condition that you have not expressed opposition to such marketing and you are entitled, at any time, to deregister from our newsletter and marketing emails. To do so, kindly contact hello@lexplore.com. or use the deregistration link stated in each newsletter/email.

Pupils tested for the assessment

Lexplore Analytics processes the following personal data about Pupils:

- Name
- Personal ID number
- Gender
- Birthdate
- Information about School and Class
- Eye Movement Recordings
- Audio Recordings
- Test results
- Comments about the Pupil

Why do we process this data?

On each test occasion the Pupil, together with a person appointed by the Customer, carries out the test by reading a text on a computer screen. The computer stores eye movement recordings and audio recordings. These are temporarily connected to a unique ID, which is automatically then uploaded to the cloud where the test is analysed.

The test results are thereafter processed in Lexplore's results portal. The Pupil's name and personal ID number are processed to ensure that the test results, i.e. reading ability, can be linked to the correct pupil. Personal ID numbers are used to ensure that all requirements for secure identification are satisfied. Data regarding the Pupil's school and class is also processed to ensure only authorised personnel within the School can access their results.

Data regarding the Pupil's gender and date of birth must be processed in order, among other things, to enable the Customer to draw conclusions regarding the Pupil's reading ability compared with other pupils. Thereby, determining whether there is a need for any special support measures.

In the Results Portal, there is a possibility for Customers to write a comment in relation to the Pupil. Comments take place in free text and may contain information regarding the implementation of the test and any circumstances which might have affected the quality.

How long do we store pupil data?

Personal data about the Pupil is processed from the time that the Pupil carries out the test until a short time after the Pupil's results are presented to the school. Lexplore stores Pupils' personal data within the scope of its tests and follow-up of the test results for as long as the Pupil is a part of the school.

If the School terminates the service or consent is revoked, the Pupil's data will be anonymised. In the event the Pupil switches to a school outside of the local authority, the Pupil's data will be anonymised.

With whom do we share personal data?

Access to the Pupil data is restricted to authorised personnel appointed by each Customer.

Lexplore Analytics transfers personal data to Lexplore AB (559069-1811 Tegelbacken Stockholm, 0702487646) Lexplore Analytics Limited (a company registered in England and Wales, company number 11121766 of Suite 8 Bowden Hall Marple, SK6 6ND) and Lexplore Nordic AB (Reg. No. 559091-9212, Tegelbacken 4A, 111 52, Stockholm).

These Lexplore Companies process Pupil's personal data on behalf of the Customer in connection with the performance of a service for the Customer. All personal data about the Pupil is encrypted when stored or processed by Lexplore Companies.

Lexplore Companies may anonymise the data collected and use in aggregation with other data to improve our Services (and the AI underlying them) for the benefit of future users. In such cases, Lexplore Analytics will be data controllers. The lawful basis on which this personal data is processed is entirely from consent (this consent may have been given by your parent or guardian). In such cases, forms should have been given to you by our Customer for you (or your parent or guardian) to sign.

Lexplore Analytics can also provide Pupils' personal data to public authorities if we are obliged to do so by law.



Your Data Protection rights

All parties have certain legal rights which can be exercised. Set forth below is a summary of these rights. For complete information regarding your rights, please see the General Data Protection Regulation, sections 3–5.

1. **Right to access/extracts from a filing system.** You are entitled to know whether Lexplore is processing personal data about you. If the answer is yes, you are entitled to information regarding, among other things, which personal data is being processed, the purposes of the processing, which external recipients receive your personal data, and how long we save your personal data.
2. **Right to data portability.** You are entitled to request a copy of the personal data which you have provided to Lexplore in a structured, generally usable, and machine-readable format. You are also entitled to request that Lexplore transfer this personal data to another controller. The right to data portability applies to data which is processed in an automated manner, and which is based on your consent or an agreement to which you are a party.
3. **Correction of incorrect data.** You are entitled to request that Lexplore correct any incorrect or incomplete information about you.
4. **Erasure** You are entitled to request that Lexplore erases all of your personal data under certain conditions, for example where the personal data is no longer necessary for the purpose for which we collected it.
5. **Right to object** You have the right to object to Lexplore's processing of your personal data. The right to make objections applies, among other things, to where or when the processing is based on a weighing of interests, unless Lexplore can prove (i) a compelling legitimate interest for the processing which overrides your interests, rights and freedoms; or (ii) where the processing is being carried out in order to establish, exercise, or defend against a legal claim.
6. **Right to object to marketing.** You have the right, at any time whatsoever, to object to Lexplore's processing of your personal data for direct marketing purposes. If you object to such processing, Lexplore must discontinue all direct marketing to you without unnecessary delay.
7. **Right to restrict.** You have the right to request a restriction on Lexplore's processing of your personal data in certain cases. If, for example, you have stated that your personal data is incorrect, you can request a restriction on the processing during a period of time which allows Lexplore the opportunity to verify whether the personal data is correct.
8. **Right to complain.** If you have any complaints regarding Lexplore's processing of your personal data, you are entitled to submit such complaint to the Privacy Protection Authority.

If you wish to submit a request for an extract from a filing system, data portability, correction, erasure, objection or restriction, please contact Lexplore at data.privacy@lexplore.com.

The Legal Basis for processing personal data in school

In order to process personal data, there must be a legal basis or valid reason for processing and saving this personal data. Consent is often regarded as the weakest legal basis, especially when schools are in a position of authority over pupils. There are certain steps schools need to consider when identifying their legal basis for processing pupils' personal data and implementing data protection policies.

School ICO Registration

As Data Controllers, schools must notify the ICO regarding the processing of personal information. As an organisation schools must register with the ICO and pay an annual fee. As part of this registration schools must notify the ICO of:

- Their purpose for processing personal data
- What data they process
- The source of the data they process
- Whom they will share the data with
- Whom they transfer the data to

School Privacy Policy

To comply with the Data Protection Act, schools need to clearly set out how they intend to use the information they collect about children, staff or parents within a comprehensive Privacy Policy, including:

- Organisational details
- The purpose and process for handling data
- Information on the methods of collection
- Details on erasure of confidential data
- Details on methods for keeping up to date
- Expectations for staff working with data
- Details on data security systems
- Details on encryption
- Procedures for lost or stolen data
- Information on trusted third parties

Security Measures in School

As well as standard and comprehensive data protection policies, there are also some simple, easily implemented measures which can be made to secure data in the classroom.

- Shredding confidential paper documents
- Installing firewalls and anti virus software
- Using strong passwords
- Keeping devices locked when not in use
- Not leaving papers lying around
- Disabling auto-complete settings online

Rights of access

Pupils, or parents and guardians acting on their behalf, have a right to request to see any personal data the school holds about them. Responding to any access requests, schools must consider whether children are mature enough to understand their rights. In such cases that they are, responses should be made to children and not their parents.

Sharing data in school

Schools may have to share pupils' personal information with local authorities, social services, other schools and departments. For sharing this information schools will need to consider all legal implications for doing so. They must also have consent from individuals before sharing information. This should form part of the school's Privacy Policy.

Keeping personal data up to date

It is essential that personal data in school is kept up to date. At the start of each school year, letters must be sent to parents and guardians to ensure that pupil details are accurate and correct. All out of date data should be securely disposed of.

Publishing exam results

The Data Protection Act does not prevent schools from publishing their exam results. However, before publishing students must be informed, including how the information will be displayed. Pupils also have a right to request a breakdown of marks and any comments. However, schools cannot disclose information relating to a pupil's individual answers.

You can learn more about data processing in school by visiting the ICO Website - [Here](#)

Lexplore Analytics and Cookies

Lexplore Analytics uses cookies and similar technologies on our websites and thereby collects certain personal data regarding persons who use our websites. In this cookie policy, we explain, among other things, which cookies we use, what they are used for, and which choices you can make about our cookies. The privacy policy also describes your rights in relation to us and how you can exercise your rights regarding the processing of your personal data.

Who is the Data Controller?

Lexplore is the controller for personal data collected on our websites. Set forth below is Lexplore's contact information.

Lexplore AB, company reg. no. 559069-1811
Fleminggatan 20, 112 26 Stockholm, Sweden
Tel: +46 (0) 702 487 646

If you have any questions regarding our handling of personal data on our website, please contact our data protection officer at data.privacy@lexplore.com.

What is a cookie?

A cookie is a small text-based file which is placed on your computer or similar unit, containing information about your navigation on the website. There are temporary cookies and permanent cookies. Temporary cookies,

also referred to as session cookies, are saved in your unit until you close the web browser. Permanent cookies have an expiration date and when this date is passed the cookie is deleted when you return to the website which created it.

Cookies may be "first-party cookies" or "third-party cookies". First-party cookies are cookies which are placed on the websites by Lexplore. Third-party cookies are cookies which are placed on the websites by another organisation, with the consent of Lexplore.

What cookies do we use?

The table below specifies the cookies which we use on our website, with information on the purpose, the type of data collected, the duration it is collected for and who handles the cookie.

Cookie	Purpose	Personal identifier	Duration	Handling	
Google Analytics	Measures the number of visitors and how the visitors navigate the website, in order to optimise the content.	IP-address	2 years	Third party	
			_gat		10 minutes
			_gid		24 hours
Microsoft Azure Application Insights	Used to develop the service. The cookie sends diagnostic and telemetric data regarding the browser session. The IP address is used in order to determine geographic region.	IP-address	Session	Third party	
			ai_user		1 years
Microsoft Azure	Used to balance the traffic to the servers, in order to improve the user's experience of the service.	non	Session	Third party	
Microsoft Azure AD B2C	Used for correct authentication at login.	B2C-ID	Session	Third party	
					b2cSignin
Amazon Web Services ALB Sticky Cookie	Used in order to be able to balance traffic correctly.	non	7 days	Third party	
Lexplore authenticating	Secures the authentication for the user session between the web browser and our server by matching a unique text string (token) to our server.	This token is matched to the username and email address in the database	Session	First party	
					idsrv
					idsrv.clients
					b2cPolicyCookie
	idsrv.session				

Hubspot	__hssc	These cookies are necessary to enable the live chat functionality. They also track and log the user's activity on the Result portal in order to improve customer satisfaction and enhanced support.	These cookies are matched either to the email address used in the chat or when signing in to the Result portal.	Max 13 months	Third party
	__hssrc				
	__hstc				
	__cfduid				
	__hluid				
	hs-messages-hide-welcome-message				
	hs-messages-is-open				
	hubspotutk				
	messagesUtk				
IDE					
Hotjar	_hjIncludedInSample	Hotjar cookie track user interaction to present relevant content.	non	Session	Third party
Youtube	GPS	These cookies are necessary to enable video content.	non		Third party
	PREF				
	VISITOR_INFO1_LIVE				
	YSC				

What is the legal basis?

Lexplore processes your personal data as set forth above based on your consent which you provide when you visit our websites.

Can I say no to cookies?

If you do not wish to allow the storage of cookies, you can normally shut this off in whole or part in your web browser's settings. In some web browsers, you can for example choose to block all cookies, only accept first-party cookies, or delete cookies when you close down your web browser. You can even delete cookies in your settings which have been previously stored.

Remember that if you choose to delete or block cookies, this may result in our websites and services not functioning.

Who do we share data with?

The data collected via third party cookies, such as IP address, will also be disclosed to the party which provides the cookie (see section 4 of the table). This type of personal data includes, among other data, your IP address and email address. These cookies are typically used by third parties in order to determine the surfing habits of the user and can ultimately be used for advertising, etc.

Lexplore may even transfer your personal data to Microsoft. This recipient is only entitled to process your personal data on behalf of Lexplore in conjunction with its performance of the service for Lexplore, for example authentication in conjunction with log in. Lexplore takes all reasonable legal, technical, and organisational measures to ensure that your data is handled securely and with an adequate level of protection when transferring to, or sharing with, such selected third parties.

Lexplore may also disclose your personal data to public authorities where we are obligated to do so by law. In the event all or part of Lexplore's business is sold, we may transfer your personal data to a potential purchaser of the business.

Transfer outside of the UK and EU

Personal data will primarily be processed within the EU/EEA area but may also be transferred to the United States. Lexplore has implemented appropriate safeguards in order to protect your personal data, through the recipient of the personal data having executed an agreement containing certain standard contract clauses which have been approved by the EU Commission. A copy of these signed standard contract clauses may be obtained upon request submitted to data.privacy@lexplore.com.

How did we review data protection policy?

In addition to the expertise of our own team, we also use external specialists in both law and data security to make sure that we meet and exceed data protection requirements.

2016: Introductory IT architecture work began for the development of Lexplore's systems and assessment. An investigation by external data security experts ensures that systems are built in accordance with Data Protection Legislation.

2017-20: As more schools across Sweden begin to use the Lexplore software, and the company moves to new markets in the UK, USA and others internationally, national lawyers and data security experts conduct in depth reviews of Data Protection Policy to make sure this meets strict national requirements and new GDPR legislation.

2016: In order to classify Lexplore's data an external expert is hired to determine whether data is to be classed as Health data. The answer is that it is not.

2020: As Biometric Data Security becomes a topic of increased attention and media interest internationally, Lexplore commissioned an independent review by experts in the field to ensure to ensure the highest levels of data protection.

2007-15: Research at the Marianne Bernadotte Centre of the Karolinska Institute in Stockholm is conducted. This is conducted in accordance with the strict guidelines, laws and / or procedures which govern research projects.

2017: An independent review of Lexplore's IT security systems is carried out. Results of this external investigation determine that the procedures that Lexplore have in place exceed all legislative requirements.

About Lexplore Analytics

Lexplore is a pioneering and mission-driven company, which provides schools with new technology and resources to promote reading development.

At the core of our offering is a ground breaking method of measuring reading attainment, which uses artificial intelligence and eye tracking technology to offer an entirely new insight into literacy.

By measuring when, where, and how a student's eyes move in relation to the words they are reading, our paperless assessment quickly analyses a their skills across key reading components, determines their attainment, and highlights potential barriers in a matter of minutes.

With immediate, fully objective and in-depth results, teachers can then work with our dedicated intervention package to support both emerging and fluent readers in their development.

Lexplore