INFORMATION SECURITY & PRIVACY DOCUMENTATION

Release May 2018

Contents

Privacy and information security is Lexer's core business

1 Executive Summary

Key points regarding privacy and information security at Lexer:

- Privacy and information security is Lexer's core business
- Lexer has a comprehensive set of information security policies
- Lexer's security credentials are subject to multiple 3rd party annual audits (incl. SOC 2)
- Lexer only has access to PUBLIC social media and web data [1]
- Lexer only sources Twitter, Facebook and Instagram data from the official API endpoints and abides by the respective terms of use
- Lexer, defined as a Data Processor, complies with GDPR
- Client data is kept confidential and is deleted on expiry of the agreement

[1] Except for authenticated communication between and client and user via Lexer Engage, which is not used for any other purpose and is only accessible by the relevant client.

2 Information Security Overview

Like many companies, Lexer faces an increasingly advanced threat environment in the area of information security. Third parties wishing to compromise the information of global companies continue to increase in number, capability, and persistence. To address this reality, Lexer has established policies which set forth Lexer's commitment to information security and privacy and define practices and procedures to be followed by Lexer personnel.

The standards of conduct that are central to Lexer's information security and privacy policies are:

- Information security management system: Lexer has and will continue to create and maintain an information security management system that complies with the requirements of ISO27001:2013.
- Risk prevention and reduction: Lexer has and will continue to evaluate information-based risks, establish information security objectives, and execute planned measures to prevent and reduce the occurrence of risks.
- Technical measures: Lexer has and will continue to implement technical measures with the aim of protecting information.
- Organizational measures: Lexer has and will continue to promote information security measures in all areas of our business activities.
- Compliance with laws: Lexer has and will continue to comply with all laws, restrictions, conventions, and internal standards pertaining to information security.
- Education: Lexer has and will continue to spare no effort in the area of education, training, and public relations exercises regarding information security. We will ensure that all employees are aware of and fully understand the Basic Information Security Policy.
- Audits: Lexer has and will continue to conduct regular information security audits, with the aim of maintaining and increasing the level of information security.
- The protection of Lexer's sensitive information, in particular that which belongs to Lexer's clients and partners, remains a global priority.

3 Information Security: Key Controls

Clients and partners entrust Lexer with their most confidential and valuable information. Lexer has developed an Information Security Management System (ISMS) and includes the key controls outlined below. Lexer's detailed ISMS is available to clients on request.

- All client and partner data is classified as RESTRICTED information
- RESTRICTED information is only stored or processed in a "red zone" facility. A red zone facility is one with minimum security standards that include physical access control lists to manage ingress and egress, security fencing, boom gates, 24 x 7 x 365 manned security, 24 x 7 x 365 CCTV recordings, pre-cast reinforced concrete building with limited entry and exit points, access control (mantraps) and biometric readers at all main entry points. Physical entry to red zone facilities must be approved by Lexer's CTO.
- RESTRICTED information is encrypted:
  - In transit using Transfer Layer Security protocol (between browsers & servers) and Secure File Transfer Protocols (between Lexer & clients); and
  - At rest using Advanced Encryption Standard AES-256.
- RESTRICTED information is used exclusively by a small number of predetermined and authorized employees. Access to network, systems, applications and information are granted to users on a need-to-know basis. Access is approved by Lexer's CTO and is controlled through the use of user IDs, strong and frequently changed passwords, multi-factor authentication and privilege settings.
- Lexer's Security team continuously monitors security systems, event logs, notifications and alerts from all systems to identify and manage threats.
- All systems used in the provision of the services, including firewalls, routers, network switches and operating systems, log information to their respective system log facility or a centralized syslog server (for network systems) in order to enable security reviews and analysis.
- Multiple layers of security controls protect access to and within our environment, including firewalls, intrusion protection systems and system segregation. Lexer's security services are configured, monitored and maintained according to industry best practice. High level system boundaries and relevant system components are documented in Appendix 3.

4 Client & Partner Data

Lexer services includes the storage and processing of client and partner data. Background into each of these areas is set out below.

Client Data

- Refer "Key Controls" section above for applicable physical security, cryptography and access controls.
- Similar to many SaaS providers, Lexer uses a top-tier, third-party data hosting provider (Amazon Web Services) with servers located in the U.S. and Australia to host our online services.
- Unless otherwise agreed in a client agreement, Lexer acknowledges and agrees that it has no rights in or title to any of the intellectual property contained in client data
- Client data will not be resold, reproduced, published externally or shared with any third party in any form or by any means in whole or in part without the client's prior written consent.
- Namespaces are used to segregate client data from other data and isolate access privileges
- Client data is permanently deleted from all Lexer systems (including backup) within 90 days of expiry or termination of the client agreement

Partner Data

- Twitter: Lexer only collects Twitter data directly from Twitter using their official API endpoints (https://developer.twitter.com/) and complies with the Twitter Developer Terms (https://developer.twitter.com/en/developer-terms). Twitter only provides Lexer with access to "public" data via the API endpoint [1].
- Facebook: Lexer only collects Facebook data directly from Facebook using their official API endpoints (https://developers.facebook.com/) and complies with the Facebook Platform Policy (https://developers.facebook.com/policy/). Facebook only provides Lexer with access to "public" data via the API endpoint [1].
- Instagram: Lexer only collects Instagram data directly from Instagram using their official API endpoints (https://www.instagram.com/developer/) and complies with the Instagram Platform Policy (https://www.instagram.com/about/legal/terms/api/). Instagram only provides Lexer with access to "public" data via the API endpoint [1].
- Web Content: Lexer licenses web content from Webhose (https://webhose.io/), a trusted web content aggregator used by global leaders for media monitoring and big data analytics. Webhose does not provide Lexer with access to any data that is encrypted or password protected.
- Linkage Data: Lexer licences linkage data from third parties including Experian (http://www.experian.com/marketing-services/targeting/data-driven-marketing/consumer-view-data.html), Full Contact (https://www.fullcontact.com/developer/enrich-api/) and Pipl (https://pipl.com/api/).
- Third Party Data: Lexer partners with a number of third party data licensors to assist in the segmentation of client data (e.g. Experian Mosaic and Mastercard)

Perhaps more important than explaining what we do do, is explaining what we don't do…. Lexer does not collect any information directly from a natural person [1], scrape websites, or harvest information from unsuspecting people using permissions hidden in apps or social login. The sources described above constitute 100% of the data that Lexer makes available as part of the Lexer services.

[1] Except for authenticated communication between and client and user via Lexer Engage, which is not used for any other purpose and is only accessible by the relevant client.

5 Privacy

Lexer is committed to meeting the privacy obligations in each of the markets in which our clients operate. A few pertinent points are as follows:

- Refer our detailed Privacy Policy here: https://lexer.io/privacy-policy/
- Lexer only stores and processes PUBLIC, "generally available" web and social media content[1].
- On the basis that:
  - Social media users are provided with security settings that provide them with full control over PUBLIC vs private content; and
  - Social media terms make it clear that PUBLIC content will be shared with developer partners such as Lexer (refer examples at Appendix 1)

  A social media user should reasonably expect that PUBLIC content (including certain Personal Information) will be collected by third party developers, including Lexer, via the official social network API endpoints. Further, the time and cost involved of collecting that public information directly from the individual to provide services such as those provided by Lexer is both unreasonable and impracticable.
- We ensure clients and partners agree (via contract) that they too comply with local privacy regulations

- Lexer isn’t signed up to Privacy Shield because it is an Australian-headquartered company (not a US-headquartered company). Privacy Shield is only one of a few available mechanisms to transfer data outside of the EU, and certification against the Privacy Shield is not a legal requirement. We rely on a combination of measures to ensure compliance with EU data export rules, including model clauses.

Refer Appendix 2 for examples of how clients describe Lexer services within their own Privacy Policies.

[1] Except for authenticated communication between and client and user via Lexer Engage, which is not used for any other purpose and is only accessible by the relevant client.

6 GDPR Compliance

Lexer is a Data Processor as defined by the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) because it processes Personal Data on behalf of clients and partners (the clients and partners are the Data Controllers as defined by the GDPR). Lexer is not a Data Controller because the purpose of processing Personal Data is determined by Lexer's clients and partners, not by Lexer. Lexer does not claim ownership of any Personal Data, nor does it facilitate the collection of any personal information directly from a natural person without instruction via agreement with a relevant Data Controller (i.e. a client or partner).

Lexer's commitment to compliance with the GDPR as it relates to Data Processors is summarised as follows:

- Lexer has appointed a Data Protection Officer. You can contact Lexer's DPO at dpo@lexer.io
- Lexer has implemented technical and organizational measures to account for security risks, which are summarised in Lexer's ISMS and subject to annual review via an internal audit and external ISO 27001 certification / SOC 2 audit.
- Lexer has a system to assist clients and partners in responding to requests of individuals
- Lexer keeps Personal Data strictly confidential and obligates personnel, partners and clients to similar confidentiality obligations by written agreement
- Lexer maintains meticulous written and system records and makes records available to clients, partners and regulators as required
- Lexer notifies clients and partners of a data breach incident within 24 hours of identification and provides persistent support
- Lexer only processes Personal Data to the extent permitted by clients and partners
- If applicable to the Service, Lexer obtains clients and partners' written permission before engaging sub-processors
- If applicable to the Service, Lexer enters into contracts with sub-processors providing the same level of protection as the principal contract with client / partner
- Lexer notifies the client / partner if their instructions infringe EU data protection laws
- If required, Lexer assists clients / partners in their Data Protection Impact Assessment
- Lexer will delete or return to the client or partner (at their request) all Personal Data when no longer providing services
- Lexer has no short-term plans to store data in the EU, and this isn’t required under GDPR. Instead, Lexer will ensure that GDPR-approved safeguards are in place before transferring Personal Data out of the EU (or confirm that the "receiving" country is on the EU Commission's list of approved countries).
- Lexer will assist clients and prospects in responding to an individual's exercise of their privacy rights
- Lexer will cooperate with requests of EU member state regulators
- Lexer has trained employees on GDPR and created company policies on compliance and non-compliance
- Lexer has updated company policies, including its online privacy policy and ISMS

- Lexer has a GDPR compliant Data Processing Addendum available for clients to review and sign at https://www.lexer.io/trust-and-compliance/dpa/.

Definitions

‘Personal Data’ means information relating to an identified or identifiable natural person (a "Data Subject") within the borders of the European Union. A person can be identified from information such as name, ID number, location data, online identifier or other factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

‘Processing’ means any set of operations performed on Personal Data, such as collection, storage, use and disclosure

7 Insurance

Lexer maintains policies for Cyber Security, Professional Indemnity and Public Liability, with certificates of currency available on request.

8 Third Party Audit & Certification

Lexer regularly evaluates the operability of its information security environment as follows:

- SOC 2 Audit (completed annually by PwC; latest report available at https://www.lexer.io/trust-and-compliance/SOC2/)
- ISO 27001:2013 Certification (completed annually by SAI Global; latest Certificate and Statement of Applicability available on request)
- Penetration and vulnerability tests (completed at least annually by Hivint Cybersecurity Consultancy; latest test results available on request)
- Internal audits (completed at least annually and reviewed as part of the SOC 2 audit and ISO Certification)

Appendix 1: Social Network Terms

Correct at the time of writing are the following Twitter, Facebook and Instagram terms that enable them to share PUBLIC data with Lexer and other developer partners.

Twitter

Tweets, Following, Lists, Profile, and Other Public Information: Twitter is primarily designed to help you share information with the world. Most of the information you provide us through Twitter is information you are asking us to make public. You may provide us with profile information such as a short biography, your location, your website, date of birth, or a picture. Additionally, your public information includes the messages you Tweet; the metadata provided with Tweets, such as when you Tweeted and the client application you used to Tweet; information about your account, such as creation time, language, country, and time zone; and the lists you create, people you follow, Tweets you Like or Retweet, and Periscope broadcasts you click or otherwise engage with (such as by commenting or hearting) on Twitter. Twitter broadly and instantly disseminates your public information to a wide range of users, customers, and services, including search engines, developers, and publishers that integrate Twitter content into their services, and organizations such as universities, public health agencies, and market research firms that analyze the information for trends and insights. When you share information or content like photos, videos, and links via the Services, you should think carefully about what you are making public. We may use this information to make inferences, like what topics you may be interested in. Our default is almost always to make the information you provide through the Services public for as long as you do not delete it, but we generally give you settings or features, like protected Tweets, to make the information more private if you want. For certain profile information fields we provide you with visibility settings to select who can see this information in your profile. If you provide us with profile information and you don't see a visibility setting, that information is public. You can change the language and time zone associated with your account at any time using your account settings, available at https://twitter.com/settings/account. (https://twitter.com/en/privacy)

Facebook

Public information is any information you share with a public audience, as well as information in your Public Profile, or content you share on a Facebook Page or another public forum. Public information is available to anyone on or off our Services and can be seen or accessed through online search engines, APIs, and offline media, such as on TV. (https://www.facebook.com/policy.php)

Instagram

Any information or content that you voluntarily disclose for posting to the Service, such as User Content, becomes available to the public, as controlled by any applicable privacy settings that you set. To change your privacy settings on the Service, please change your profile setting. Once you have shared User Content or made it public, that User Content may be re-shared by others. Subject to your profile and privacy settings, any User Content that you make public is searchable by other Users and subject to use under our Instagram API. The use of the Instagram API is subject to the API Terms of Use which incorporates the terms of this Privacy Policy. (http://instagram.com/legal/privacy/)

Appendix 2: Privacy Policy Examples

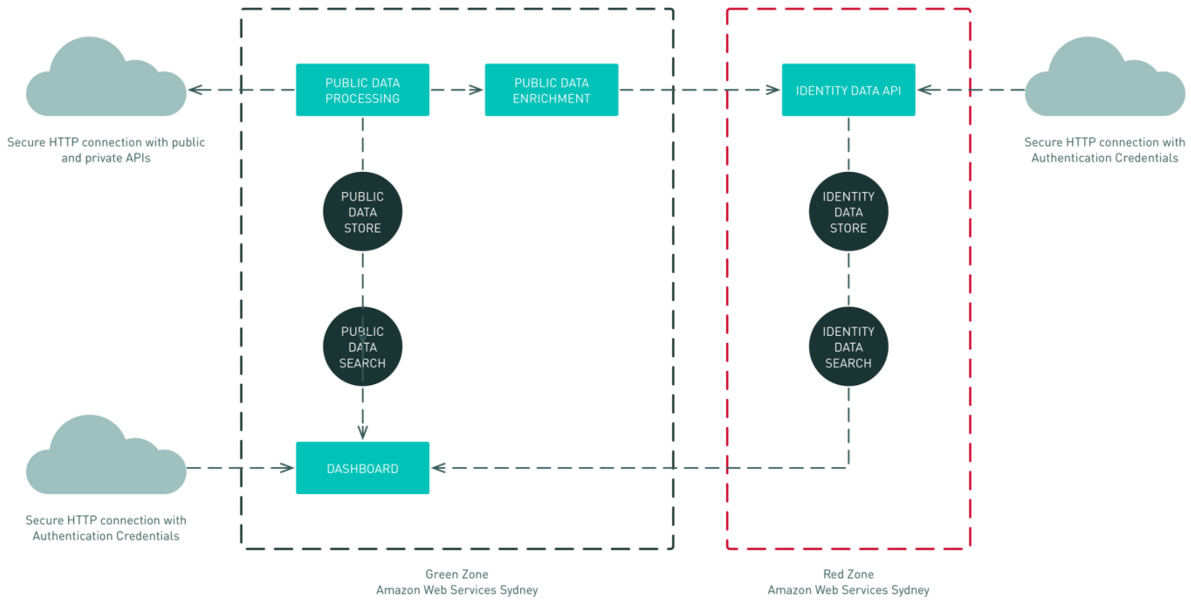
THE FOLLOWING IS NOT INTENDED TO BE COMPREHENSIVE NOR DOES IT CONSTITUTE LEGAL ADVICE. YOU SHOULD SEEK LEGAL OR OTHER PROFESSIONAL ADVICE BEFORE ACTING OR RELYING ON ANY OF THE CONTENT.

For information only, set out below are some provisions that have been included by global Lexer clients in their Privacy Policies to describe how they work with Lexer.

- "Who we work with: We work with a number of third party companies, and in certain circumstances may share personal information with them. In these circumstances, we have arrangements in place with our partners that limit their use or disclosure of your personal information to the agreed purpose only."
- "What we collect from others: We may collect personal information from other companies that are able to disclose it to us, if it's not practical to collect it from you. For example, we buy or obtain personal information from trusted sources to help us identify people who might be interested in hearing about our products."
- "Advertising: Everyone hates being bombarded with ads for things they don't need or have any interest in. We may use your personal information to send you advertising that is customised or more relevant to your interests, characteristics or general location. This doesn't necessarily mean you'll get more advertising. It just means that the advertising that you see will hopefully be more relevant to you."
- "Insights from statistics and research: We aggregate, combine and process personal information to generate new insights about our products and customers, so we can provide you with the best possible service."

Appendix 3:

High level system boundaries and relevant system components are as follows:


PUBLIC DATA PROCESSING
PUBLIC DATA ENRICHMENT
IDENTITY DATA API
PUBLIC DATA STORE
PUBLIC DATA SEARCH
IDENTITY DATA STORE
IDENTITY DATA SEARCH
DASHBOARD
Secure HTTP connection with public and private APIs
Secure HTTP connection with Authentication Credentials
Secure HTTP connection with Authentication Credentials
Green Zone
Amazon Web Services Sydney
Red Zone
Amazon Web Services Sydney