INFORMATION SECURITY & PRIVACY DOCUMENTATION

Release February 2020

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 provides services to a number of leading enterprises, including telcos, banks, insurers, miners and retailers
- Lexer has never had a security breach
- Lexer has never failed an audit or test – ISO 27001, SOC 2, pen tests, internal audits and client reviews
- All data stored and processed at either AWS Australia (for Asia Pac clients) or AWS USA (for US clients)
- All data encrypted in transit and at rest
- Information is only accessed on a "need to know and least privilege basis"
- Access is controlled using strong passwords and multi-factor authentication
- All systems are subject to continuous scanning and logging (anti-virus, intrusion protection etc)
- We will not do anything with client data except deliver the services as per the agreement
- Client data is kept confidential and is deleted on expiry of the agreement

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 Secure File Transfer Protocols (SSH2 asymmetric cryptography, IP whitelists and secure storage / rotation of API keys using AWS Secrets Manager); 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 1.
- Processes are in place to identify threats and vulnerabilities, monitor critical patch notifications and install patches immediately upon release.
- Client access to the Lexer platform is secured using Okta and includes a combination of strong passwords (8 digit, upper, lower, number), lock out (5 attempts, 3 minutes), multi-factor authentication (SMS or Google Authenticator) and SSO (SAML 2.0).

4 Client Data

Lexer services includes the storage and processing of client data as follows:

- 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

5 Privacy & GDPR Compliance

Lexer is committed to meeting the privacy obligations in each of the markets in which our clients operate, including GDPR, the Australian Privacy Act (1988) and the **California** Consumer Privacy Act. Refer our detailed Privacy Policy here: https://lexer.io/privacy-policy/

GDPR

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 summarized 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 summarized 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, including but not limited to where individuals have exercised a right to have personal data erased ("right to erasure/right to be forgotten") whereby Lexer will erase all personal information from Lexer systems, including backups, within 3-weeks of receiving a written request from the relevant client or prospect.
- 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

6 Insurance

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

7 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:

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