	CILEx Regulation Limited
Date	**24 February 2022**
Item	**16.0**
Title	**Information Governance Annual Review**
Authors	**Patricia Morrissey, Interim Director of Governance**
Purpose	To report on key activity, achievements and issues relating to Information Governance in 2021
Recommendation	The Board is invited to **APPROVE** the report
Timing	N/a
Impact assessment	This report provides assurance to consumers, regulated members and other stakeholders that we are meeting our obligations under data protection legislation
Appendices	None
For publication	Yes

Introduction

1. The purpose of this report is to ensure the Board is aware of key activity relating to Information Governance within CILEx Regulation Limited. This is the third Information Governance (data protection) annual report to be presented to the Board.

2. The report reviews our activity around data protection during 2021. Our approach in 2021 has been more reactive than previous years due to ongoing challenges, including staff capacity and the pandemic. In light of this in 2021 we have focused on dealing with key priorities, mainly Subject Access Requests.

Background

3. The implementation of the General Data Protection Regulations (GDPR)[1] and subsequent Data Protection Act 2018 introduced stricter requirements in how organisations handle personal data with significantly higher penalties applicable for serious failings. In addition, the introduction of this legislation has resulted in greater public awareness of how organisations must behave, bringing with it higher risks of legal challenge and reputational damage.

Understanding Risk

4. We are very conscious of the potential effect on our reputation as a legal regulator if we are accused of mishandling personal data and thereby breaching data protection law. Even if an accusation is unfounded, the potential damage would still be problematic, particularly if the complainant uses social media to air their grievance.

[1] Now UK GDPR

5. CILEx Regulation handles complex personal data, including special category data, to fulfil our purpose and regulatory objectives. We require a different legal basis for processing data for different membership grades and interpreting this has required external legal advice on two occasions during 2021.

6. We have a named Data Protection Officer, in-line with GDPR, Clare Harper Smith.

Key issues for consideration

Compliance assessment

7. No high or medium level compliance information governance issues have been identified.

8. In 2019, for the first time, we introduced using an external consultant to carry out a high-level independent view of our information governance compliance. The 2019 external assessment did not identify any major gaps in our information governance arrangements at that time and our intention was to invite external review every three years with the next review during 2022. Given our current priorities, we are considering the best way to proceed in terms of the timing and focus of any review.

9. We have a positive staff culture with a good understanding of the importance of data protection. Staff have consistently shown a willingness to ask questions, learn and take responsibility for the protection of personal data and have felt able to speak up promptly if they believe they may have made a mistake. Periodically, data protection reminders are raised at staff meetings, particularly in relation to email security/ data breaches, this has been particularly important during the pandemic with the increase in cyber attacks and phishing scams.

10. Staff undertake annual refresher training in data protection and information security and completion rates are monitored via monthly performance figures. The December 2021 figure for compliance was 95% compared with 100% in November and reflects staff joining the organisation.

Data protection statistics

Data breaches

11. There have been three data breaches in 2021 compared with four in 2020. None were the more serious level of breach that requires reporting to the Information Commissioner.

12. In two cases, the data breaches related to personal information being sent to the wrong recipient and one to information being sent to a mistyped email address.

13. In all three cases, the breaches were due to human error and were raised as soon as staff became aware of them, and steps taken to mitigate any effects. The personal data was assessed low risk in all instances.

14. In the three cases, no system or process improvements were identified. Staff are all up-to-date on both data protection and information security training plus staff are regularly reminded about e-mail security. All staff were reminded at a staff meeting of the importance of double-checking email recipients.

Complaints

16. We received no complaints in 2021 relating to data protection.

Subject Access Requests (SARs)

15. We received six SARs in 2021 compared with three in 2020 and nine in 2019. Of the 2021 SARs, two were received from CILEX as part of a group-wide requests and four related to Enforcement investigations (two of which related to the same investigation). The use of SARs by both parties (complainant and member complained against) has been a noticeable feature since the GDPR came in.

Erasure requests

16. During 2021, we received two erasure requests via CILEX. CILEx Regulation held no information on one requestor, and a very small amount of information on the second relating to reminders about CPD compliance which we deleted.

Freedom of Information requests

17. We are not subject to the Freedom of Information Act. Therefore, whilst we endeavour to be helpful to public enquiries, we do not collect statistics on these types of enquiries.

Data Protection Improvements delivered in 2021

18. Since the Board's last report, we have:

- Developed our own independent set of data protection policies with particular emphasis on Data Protection policy and Retention, Archiving and Destruction policy.

- Added data protection duties to job descriptions. Additionally, the Data Protection Officer has also been given the right of access to the Chair of the Board on data protection issues of concern.

- Introduced two-factor authentication (2FA) for enhanced information security for all staff.

- Introduced a separate annual training course in Information Security in addition to GDPR. Compliance was 100% in November and 90% in December.

Focus for 2022

19. As a data controller, we carry significant responsibility under GDPR for the data supplied to third parties as our data processors. In 2022 we will be exploring online Data Protection training for panellists and Board members.

20. Following the departure of the Director of Policy, Governance and Enforcement, we reviewed the role and are looking to recruit a qualified lawyer with regulatory experience to improve our access to in-house legal support. Re-focussing this role has, in part, resulted from having to seek specialist advice on data protection matters relating to membership grades and exemptions under GDPR legislation.

Conclusion

21. CILEx Regulation, working in conjunction with CILEX as our provider of support services, continues to develop strong working practices around data protection. There are no significant information governance compliance issues to highlight to the Board. We can demonstrate robust monitoring and logging of our information governance arrangements. Staff are fully engaged with the importance of data protection and contribute on an ongoing basis to related improvements.

Recommendation

22. To Board in asked to note and **APPROVE** the report.