A Compliance Checklist for CISOs

1 IDENTIFY APPLICABLE REGULATIONS:

- Determine relevant data protection and privacy regulations for your industry, such as GDPR, NIS2, PCIDSS and DORA. ☐
- Thoroughly understand the provisions and obligations outlined in the identified regulations. ☐

2 CONDUCT A RISK ASSESSMENT:

- Evaluate your organisations current data protection and privacy practices against regulatory requirements. ☐
- Identify areas where current practices do not meet regulatory standards or where gaps exist in compliance efforts. ☐
- Develop a detailed action plan to address identified compliance gaps, including specific tasks, responsible parties, and timelines. ☐
- Establish a system for ongoing monitoring of compliance efforts to ensure adherence to regulatory requirements. ☐

3 PROVIDE EMPLOYEE TRAINING:

- Provide comprehensive training to employees on legal requirements and compliance expectations related to data protection and privacy. ☐
- Offer tailored training modules for employees handling sensitive data or involved in data processing activities. ☐

4 IMPLEMENT RESPONSE PLAN:

- Develop and implement an effective response plan to address potential regulatory violations promptly and appropriately. ☐
- Designate individuals or teams responsible for initiating and managing the response plan in case of data breaches or regulatory non-compliance incidents. ☐

MetaCompliance®
Make it personal.

5 RECORD RETENTION SYSTEM:

- Establish a systematic approach to retaining records in accordance with regulatory requirements, ensuring data integrity and accessibility.

6 CONDUCT INTERNAL AUDITS:

- Conduct regular internal audits to assess and verify continued compliance with data protection and privacy regulations.
- Review audit findings and recommendations with relevant stakeholders to drive continuous improvement in compliance practices.
- Document all compliance efforts and improvements made, including policies, procedures, training materials, and audit reports.

7 STAY UPDATED WITH LAW CHANGES:

- Regularly review changes in relevant laws and regulations to ensure compliance efforts remain up to date.
- Adjust the compliance program as necessary based on changes in laws, regulations, or business structure.

8 PREPARE FOR EXTERNAL AUDITS:

- Prepare for and cooporate with external audits and regulatory inspections, maintaining transparency and providing necessary documentation.

By following this comprehensive checklist, you can establish and maintain robust data protection and privacy compliance practices in alignment with regulatory requirements. Regular updates and continuous improvement efforts will help your organisation stay ahead of evolving regulatory landscapes and protect sensitive information effectively.