THE EUROPEAN LOTTERIES
FOR THE BENEFIT OF SOCIETY

Reference Risk Card: UNDULY USE OF PERSONAL DATA

Element ID	Risk Element	Concern
Unduly use of personal data	It focuses on the analysis of the risks to the confidentiality, integrity and availability of all personal data related to the organisation of gambling and defines its information security expectations and controls in a way that provides an appropriate response to the risks that threaten the achievement of its objectives. A personal data breach may put data subjects' rights and freedoms at risk. This can include physical, material or non-material risks.	▪ Financial impact ▪ Negative reputational impact ▪ Data protection fine by the authority ▪ Data protection authority proceedings

Unduly use of personal data risk refers to the potential threat of inappropriate or excessive exploitation of personal information that one may share with an organization or individual. This risk arises when individuals or organizations collect, process, or share Personally Identifiable Information (PII) without obtaining the necessary consent or for purposes beyond what is justified and in violation of privacy laws. The unduly use of personal data may result in identity theft, financial fraud, reputational damage, discrimination, or other adverse consequences. Therefore, Lotteries must employ robust security measures, including data encryption, access controls, and monitoring tools, to mitigate unduly use of personal data risks and comply with privacy regulations.

Frameworks/Methodologies/Standards/Tools (More relevant ones)

ISO 27001 Information Technology Security
ISO 27701 Security Techniques. Extension To ISO/IEC 27001 And ISO/IEC 27002 For Privacy Information Management. Requirements And Guidelines
Data protection laws
Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. This text includes the corrigendum published in the OJEU of 23 May 2018

Key Risk Control (Broad) Actions (KRC–Actions)			
Area	Generic		Lottery/Gaming Specific Aspects
	Objective/Action	Outcomes	
	▪ The organisation must have an appropriate IT and data protection policy. ▪ Regular IT security audits. ▪ Assessment and updating of personal data processing related to the organisation of gambling within the organisation. ▪ Annual assessment of the processes that handle personal data. ▪ A defined clear company culture should be in place to make the employees aware of the behaviours that is required in the personal data processing. ▪ Establish an appropriate data protection incident handling procedure. ▪ Provide general and departmental information security and privacy awareness at regular intervals.	▪ IT and data protection policy. ▪ Information security and privacy training plan. ▪ Security and privacy testing. ▪ Data Protection Officer. ▪ Processes for personal data list. ▪ Personal data incident management policy. ▪ ISO27701 The Standard for Privacy Information Management certificate. ▪ Comply audit report of GDPR. ▪ Risk assessment report of all procedures in the organization related to personal data. ▪ Monitoring of critical systems report. ▪ Transfer of sensitive data Policy.	

Key Performance Indicators (KPI) (Radar Diagram)	Means of Assessments of Controls and Management Effectiveness
	Self–assessment Peer assessment Second party assessment Accredited third party assessment EL Certification (eventually)


THE EUROPEAN
LOTTERIES
FOR THE BENEFIT OF SOCIETY