



Unduly Use Of Personal Data

WHAT IS THIS RISK ABOUT?

Risk of unduly use of personal data focuses on the analysis of the risks related to 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.

WHY SHOULD YOUR LOTTERY BE CONCERNED?

- Financial impact
- Negative reputational impact
- Data protection fine by the authority
- Data protection authority proceedings

HOW TO MINIMISE THIS RISK?

Actions (best practices) presented herein could be implemented to minimise risk and ensure more effective risk management.

- 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.

MAIN QUESTIONS TO KNOW THE STATUS OF YOUR LOTTERY IN RELATION TO THIS RISK

Questions/Answers

- *YES: It is implemented in your lottery*
- *NO: It is not implemented in your lottery*
- *PARTIALLY: It is partially implemented*

Have you implemented IT and data protection policies?	Yes/partially/No
Do you have trainings and testings on information security and privacy?	Yes/partially/No
Is there a designated Data Protection Officer?	Yes/partially/No
Have you identified processes that handle personal data?	Yes/partially/No
Do you have personal data incident management policy?	Yes/partially/No
Does the company have ISO27701 Standard for Privacy Information Management certificate?	Yes/partially/No
Does the company comply with the General Data Protection Regulation?	Yes/partially/No
Do you have risk assessment of all procedures in the organization related to personal data?	Yes/partially/No
Is there a policy for monitoring of critical systems and transfer of sensitive data?	Yes/partially/No