Report of the State Comptroller of Israel |
December 2025

Ministry of Defense

# Management and Security of Databases in the Ministry of Defense

# Management and Security of Databases in the Ministry of Defense

## Background

The Ministry of Defense plays a central role in achieving the State of Israel's national security objectives and, in carrying out its missions, makes use of extensive databases, including those of employees, suppliers, clients, Israel Defense Forces (IDF) disabled veterans, bereaved families, IDF casualties, freed hostages, and consultants. These databases contain personal data, such as data on an individual's character, personal status, health condition, financial status, and professional qualifications. Disclosure of the data from these databases could infringe on the right to privacy of the individuals whose sensitive information is stored in them, a right that is among the most important human rights in Israel. In addition, such disclosure could have implications for the functioning of the Ministry of Defense and for state security, as described below.

## Possible Implications Resulting from the Disclosure or Disruption of the Ministry of Defense's Databases


The risks to privacy protection and to data security in the Ministry of Defense's databases have increased since the outbreak of the Swords of Iron War, in light of the intensification of

cyberattacks, which are an integral part of modern warfare. These have included attacks on the databases of public bodies and an increase in phishing attempts targeting entities in Israel, including former members of the defense establishment. Such attempts have become more sophisticated and more focused on the target, by gathering preliminary information regarding the target's occupation and fields of interest. In 2024, there was a 24% increase in the number of cyber incidents verified by the Israel National Cyber Directorate compared with 2023 (17,078 cyber incidents in 2024, compared with 13,040 in 2023). The most common attacks were phishing incidents: in 2024, 10,084 such incidents were verified, compared with 3,301 in 2023; 44% of phishing incidents in 2023 (1,449 incidents) occurred from October 7 through the end of 2023. In addition, 1,771 incidents of intrusion into computer systems were verified in 2024, compared with 1,714 in 2023; half of these incidents in 2023 (873) occurred from October 7 through the end of that year.

The materialization of the risks to the Ministry of Defense's databases could, for example, result in the disclosure of personal data about soldiers injured in the war (the database of IDF disabled veterans) or about former hostages from the October 7 massacre who were released from Gaza (the database of freed hostages) and who, against their will, became subjects of public interest. In addition, disclosure or disruption of information from security-importance databases – such as the Ministry of Defense employee database and the Ministry's supplier database, whose confidentiality must be maintained – could impair the Ministry's functional continuity and its ability to provide the Israel Defense Forces with the required means, cause it reputational damage, harm its relations with suppliers and clients, and expose it to fines. Moreover, this matter carries psychological implications: it could even sow panic and a sense of insecurity among the public, and harm Israel's foreign relations in security and diplomatic contexts.

Indeed, since the outbreak of the Swords of Iron War, the risk of a data leak from the Ministry of Defense has materialized: in April 2024, the media reported that data from the Ministry of Defense's administrative portals had been leaked by hostile actors and published on a website established by international hackers. This included identifying information on Ministry employees, information on defense tenders, and on Israel Defense Forces technological systems, such as details about armored vehicles, engineering blueprints, and technical information on satellite imaging systems.

## Key Figures

**14**

The number of databases containing personal data[1] registered by the Ministry of Defense in the Database Public Registry; 8 of which (57%) are subject to a high level of security due to the security risks they pose

**2.84 million people**

contained in the Ministry of Defense's databases containing personal data, including 230,000 individuals whose details are listed in the IDF Disabled Veterans database, which holds data on their health and economic status, their family members, the services provided to them, etc., 18,000 of them injured in the Swords of Iron War

**18 years have passed**

since the Ministry of Defense last conducted a comprehensive mapping of all the databases it controls (2007), to determine whether it was subject to additional requirements under the Privacy Protection Law; hence, it may control additional databases

**0**

The number of risk assessment surveys conducted by the Ministry of Defense to identify data security risks in the databases, and the number of penetration tests to database systems carried out to protect them from external and internal threats

**Up to NIS 320,000**

The amount of the administrative financial fine for each high-security-level database to which the Ministry of Defense could be exposed for failing to conduct risk assessment surveys and penetration tests, upon the entry into force of Amendment No. 13 to the Privacy Protection Law

**7 out of 10**

external users[2] with access authorization to the Ministry of Defense's central computer network had not logged into the network for more than six months; 60% of them had not logged in at all. 90% are outsourced workers. Accordingly, there is a risk that they hold network access authorization without need

**60%**

of the external users who had not logged into the network for more than six months are affiliated with five Ministry of Defense departments, where the risk of exposure of security-related information, or information regarding individuals is high

**5 out of 10**

external users with access authorization to the database system managing the IDF Disabled Veterans database had not accessed the system for more than six months. Accordingly, there is a risk that they hold access authorization to the database without need

1 Such as information on an individual's personality traits, personal status, health condition, financial status, and professional qualifications.

2 The Ministry of Defense's computer systems users are divided into two groups: (a) Internal users – users whose personal details are managed in the Ministry of Defense's human resources systems, including Ministry employees, consultants, national service volunteers, and Israel Defense Forces soldiers serving in the Ministry; (b) External users – users whose personal details are not managed in the Ministry's human resources systems, including outsourced workers, employees of defense industries, and IDF users.

# Audit Actions

From August 2024 to January 2025, the State Comptroller's Office examined how the Ministry of Defense manages the databases under its control and how it secures them, in light of the provisions of the Privacy Protection Law, 1981, and the Privacy Protection Regulations (Data Security), 2017. It should be noted that the audit did not address the cyber aspects of information security. The audit was conducted in the Ministry of Defense – in the Applications and Technology Department ("the Applications and Technology Department") and the Security Department; in the Ministry of Justice – in the Privacy Protection Authority. Supplementary examinations were conducted in the Rehabilitation Department of the Ministry of Defense.

It should be noted that since Amendment No. 13 to the Privacy Protection Law will enter into force in August 2025, after the audit's completion date, the Ministry of Defense's activity was examined according to the provisions of the Law prior to the amendment, and in alignment with the requirements that will apply to it on a forward-looking basis. Accordingly, the definitions, terms, and recommendations presented in this report with respect to the Privacy Protection Law and the Privacy Protection Regulations (Data Security) are consistent with Amendment No. 13 to the Law.

# Key Findings

**Compliance of the Ministry of Defense with Requirements for Data Security in Databases (Privacy Protection Aspects)** – The Ministry of Defense's Applications and Technology Department has not fulfilled its responsibility to ensure compliance with the privacy protection requirements applicable to the Ministry regarding data security in its databases. These requirements include establishing a data security procedure, conducting risk assessment surveys, penetration tests and training sessions to raise employee awareness. Instead, the Applications and Technology Department has relied on the Security Department, which is the professional authority for data security in the Ministry, without verifying that the actions taken by the Security Department address all the unique requirements relating to privacy protection. It should be noted that the Security Department does implement measures for securing information; however, these measures are intended to secure classified information as defined in the Regulation of Security in Public Bodies Law, 1998, under which the Department operates, and they do not fully address data security requirements for databases from a privacy protection perspective.

Failure to comply with the data security requirements prescribed in the Privacy Protection Regulations increases the risks to the databases, including data leaks, data disruptions and impairment of its availability, particularly given the unique challenges of enforcing privacy protection in computerized databases. In recent years, data has leaked from the Ministry of Defense both as a result of cyberattacks by hostile external actors, who exfiltrated data from the Ministry's administrative portals – including Ministry employees' identifying data, details of defense tenders, and information on Israel Defense Forces technological systems such as engineering blueprints and technical data[3]; and as a result of human error on the part of employees who inadvertently published ID numbers, names, and vehicle registration numbers of senior Ministry of Defense officials[4].

- **The Supervision of the Ministry of Defense on the Implementation of the Privacy Protection Regulations (Data Security) in Its Databases** – Contrary to the requirements of the Privacy Protection Law and its Regulations, according to which a Data Security Officer of databases will be appointed and will regularly monitor the compliance with Data Security Regulations, there is no position within the Ministry of Defense tasked with identifying the requirements applicable to the Ministry under the Law and the Regulations, validating compliance with them, and supervising their implementation. Furthermore, up until October 2024, the Head of the Applications and Technology Department of the Ministry of Defense – who is tasked with managing the Ministry's databases and, by law, bears direct responsibility for the security of the data in them as well as for meeting the obligations outlined in the Regulations regarding the databases controlled by the Ministry – did not ensure that the Data Security Officer fulfilled her duties as required by the Regulations. Consequently, he did not monitor the Ministry's compliance with the applicable requirements, despite the importance of these Regulations for protecting the privacy of individuals whose sensitive information is stored in the databases, and despite the significant risks these databases are exposed and their far-reaching implications for individuals, the organization, and national security.

- **Mapping and Registering the Databases of the Ministry of Defense** – Contrary to the requirements of the Privacy Protection Law, according to which a database controller will register these databases in the Database Public Registry and notify of certain changes relating to them, the Applications and Technology Department has not mapped all data controlled by the Ministry of Defense since 2007 to determine whether it contains personal data as defined in the Law and the Regulations, and whether

3 As reported in the media in April 2024 (for example, Israel Hayom, "Hackers Penetrated Ministry of Defense Systems: Concern That Sensitive Information Was Leaked" (April 9, 2024) https://www.israelhayom.co.il/tech/tech-news/article/15573329). The Ministry of Defense informed the media that a non-sensitive website had been breached, and confirmed this statement to the State Comptroller's Office in December 2024, as well as providing the investigation conducted following the incident and the measures taken to address the security breach.

4 As reported in 2022 in the media (for example, TheMarker, "A Small Excel Error Exposed Details of Senior Ministry of Defense Officials Online" (August 24, 2022) https://www.themarker.com/captain-internet/2022-08-24/ty-article/.premium/00000182-cf9f-d1de-a7c3-dfdf3bca0000). The Ministry of Defense confirmed the details to the State Comptroller's Office in September 2024.

additional legal requirements – such as registering such data in the Database Public Registry – apply to the Ministry.

As a result, the Ministry of Defense has not recognized that it may control additional databases for which it is required to act under the provisions of the Privacy Protection Law and the Regulations, including databases containing sensitive personal information such as data concerning a person's family life; medical information; criminal record; salary data; religious beliefs; ethnic origin; assessment of essential personality traits, including character, intellectual capacity, and work performance; their location and traffic data.

Sensitive personal information of this kind may be included, for example, in the Ministry of Defense's databases of reliability and security clearance evaluations conducted for all population sectors employed by the Ministry, as well as in its databases of professional evaluation tests for prospective employees. Accordingly, the Ministry is not aware that it may be subject to additional obligations regarding personal data controlled by it, as well as obligations under the Privacy Protection Regulations (Instructions for Data that was Transferred to Israel from the European Economic Area), 2023. Compliance with these obligations facilitates trade relations with the EU member states, and failure to comply may harm foreign relations with defense establishments that are very important for achieving the State of Israel's national security objectives.

**Classification of Databases and Formulation of Means Intended to Protect Them** – Contrary to the requirements of the Privacy Protection Regulations (Data Security), according to which a database definition document shall be prepared describing its key aspects and each database shall be classified according to the level of security risk it poses, the Applications and Technology Department of the Ministry of Defense has neither prepared such a document for each database under its control nor classified the databases according to the applicable security levels (medium or high). As a result, the Applications and Technology Department lacks a complete and up-to-date picture of all the databases it manages, that would enable it to formulate the means intended to Protect them according to the risks each database poses. Furthermore, beginning in August 2025, with the entry into force of Amendment No. 13 to the Privacy Protection Law, the Ministry of Defense is liable to be exposed to administrative financial fines ranging from NIS 20,000 to NIS 320,000 for various violations of the Data Security Regulations vis-à-vis each database.

**Management of Access Authorizations in the Identity Management System[5]**

- The audit found that, according to an analysis made by the State Comptroller's Office, 7 out of 10 external users with access permission to the Ministry of Defense's central computer network – which serves as a gateway to databases – had not

5 A computerized system in which user accounts are managed for roles with different access permission to the Ministry of Defense's computer networks, data systems and the databases linked to them.

logged into the network for more than six months; most of them (60%) had not logged in at all. This raises concerns that these users hold access permission that is not required for the performance of their duties. The audit further found that most of the users who had not logged into the network for more than six months (90%) were outsourced employees, and a large share of them (60%) were assigned to five departments, from which the potential risk of exposure of defense-related or personal data is high. Since this network serves as the gateway to databases, and contains assets – some of them are sensitive – as well as inputs that serve processes related to IDF business operations and procurement, the risk of personal data being exposed to unauthorized individuals is heightened.

- The audit further found that the Applications and Technology Department of the Ministry of Defense had not established a reporting mechanism for entities requiring authorization from the Ministry of Defense and IDF directorates to report the end of external users' service, in order to revoke their access authorizations. This is despite the fact that, due to the absence of a structured reporting mechanism, there are active but unnecessary access permissions within the external users group, including authorizations for computer networks and data systems that serve as gateways to databases.

- The audit also found that the Applications and Technology Department does not conduct a structured and systematic permission review on the thousands of users managed in the Identity Management System and the tens of thousands of authorizations' types it contains in order to update user lists. Instead, it occasionally performs targeted, manual examinations of access authorizations for a limited group of users, at its discretion. This does not comply with the Regulations' requirement to maintain an up-to-date record of users and the permissions granted to them for the performance of their duties, despite the Department being aware of unnecessary authorizations in the external users' group.

**Management of Access Authorizations to the Disabled IDF Veterans Database**

- The audit found that, according to an analysis made by the State Comptroller's Office, 5 out of 10 users with active access permission to the Shemesh system[6] (263 out of 481 users) had not logged into the system for more than six months. Of these, 29% (78 users) had not logged in at all. This raises concerns that they hold access permission without a functional need.

- The audit further found that the Ministry of Defense's Applications and Technology Department had not established a structured reporting mechanism for entities requiring authorization to report the end of external users' service in the Shemesh system, in order to revoke their access. This is despite the fact that, due to the absence of a structured reporting mechanism, there are external users who have

6 The Rehabilitation Department's central information system, which is linked to the Disabled IDF Veterans database.

active access permissions for Shemesh-system that are not required. For example, unnecessary active permission existed for workers employed via an external supplier, such as the Rehabilitation Department's call center which employs dozens of workers with high turnover, as well as for external contractors able to connect remotely to the Shemesh system, even after their service had ended.

As a result, under certain circumstances, unauthorized parties may be exposed to personal data, including particularly sensitive data, in the Ministry of Defense's Disabled IDF Veterans Database, which contains details on more than 230,000 individuals, including their health and economic status, family members, and the services provided to them. This risk is heightened by the addition of approximately 18,000 wounded individuals to the database due to the Swords of Iron War, and the resulting increase in the number of service providers in the Rehabilitation Department who use the Shemesh system. Once Amendment No. 13 to the Privacy Protection Law enters into force, the Privacy Protection Authority will be authorized to impose administrative financial fines on the Ministry of Defense for failing to revoke user access authorization immediately upon the end of their service, to the sum of NIS 160,000 for each high-security level database, such as the Disabled IDF Veterans Database.

- **Database Security Procedure** – The Applications and Technology Department has not established a database security procedure as required by the Regulations. Certain topics that must be included in such a procedure are addressed in procedures set by the Security Department, such as cyber security incident management, secure usage of portable devices and password policy, which forms part of the access policy for the databases. However, topics such as the risks to which the databases are exposed, the manners in which these risks are identified and dealt with, and the manners of monitoring the use of the databases are not addressed in procedures of any entity within the Ministry of Defense.

  In the absence of a database security procedure, the Ministry of Defense lacks a structured and comprehensive security policy for addressing the security risks to which the data in its databases is exposed, as well as a tool for conducting periodical audits to verify the existence of security measures required under such a procedure and their proper functioning.

- **Risk Assessment Surveys and Penetration Tests** – The Applications and Technology Department has not conducted risk assessment surveys to identify data security risks in the Ministry's high security level databases, nor has it performed penetration tests to the systems of these databases to assess their resilience against internal and external threats, as required by the Privacy Protection Regulations (Data Security). While the Applications and Technology Department and the Security Department do carry out risk assessment surveys and penetration tests for various Ministry of Defense networks, database systems, and Ministry of Defense websites

developed by external contractors, to detect potential vulnerabilities, no entity within the Ministry of Defense has conducted dedicated risk assessment surveys or penetration tests for the 14 databases controlled by the Ministry. The Ministry has not identified, analyzed or assessed possible scenarios for the occurrence of security incidents in these databases – whether individually or at stages of the business processes relating to them – nor estimated the likelihood of such scenarios materializing; it has not relied on a mapping of the characteristics of the database systems that process data from the databases, or included a mapping of the existing controls in the organization against those that should be implemented to minimize the likelihood of the risks materializing. As a result, the Ministry has not examined the need to update the database definitions document or the database security procedure, has not determined the necessary controls, and has not assessed the effectiveness of the existing controls and protection mechanisms.

In the absence of risk assessment surveys and penetration tests for its databases, the Ministry of Defense lacks the tools to assess its maturity level in addressing threats to the integrity, confidentiality, and availability of the data stored in the databases; to identify weaknesses in data security; to prioritize the handling of these risks; to understand the controls it must implement in its work plans; and to evaluate the effectiveness of the controls and the existing defense mechanisms.

**Appointment of a Data Security Officer for the Ministry of Defense's Databases** – Following this audit, in October 2024 the Head of the Applications and Technology Department appointed a new Data Security Officer for the Ministry of Defense's databases and granted her powers and responsibilities in line with the Data Security Regulations. Until then, the Head of the Applications and Technology Department had not ensured that the Ministry's Data Security Officer was fulfilling her duties as required.

**Database Mapping** – Following the audit, in December 2024, the Head of the Applications and Technology Department instructed the heads of the Ministry of Defense's departments and units to map the databases within their respective departments and units. It should be noted that his directive applied only to data transferred from the Ministry of Defense to external entities or received from them. As of the end of the audit, in January 2025, the mapping had not yet been completed.

# Key Recommendations

- The Ministry of Defense should comply with the privacy protection requirements applicable to it under the Law and the Regulations, particularly in light of Amendment No. 13 to the Law, which will enter into force in August 2025 and align the legislation with contemporary challenges. In addition, given the findings from the State Comptroller's data analysis, it is recommended that the Ministry review its authorization management processes across all database systems connected to its databases. It is further recommended that the Director General of the Ministry of Defense regulate the division of responsibilities and authorities between the Applications and Technology Department and the Security Department in the field of database data security from the privacy protection perspective. This will help reduce the risks of privacy violations and of impairing the Ministry of Defense's ability to fulfill its mission.

- The Head of the Applications and Technology Department – tasked with managing the Ministry of Defense's databases – should ensure that the Data Security Officer for these databases is capable of fulfilling her role as required, that she receives the necessary training, and that the necessary resources are allocated to the task. The Data Security Officer for the Ministry of Defense's databases should carry out her role as stipulated in the Regulations, including preparing a plan for ongoing monitoring in regard to compliance with the Regulations' requirements, implementing this plan and notifying all relevant stakeholders of the findings. The Director General of the Ministry of Defense should appoint a Privacy Supervisor, as mandated by Amendment No. 13 to the Privacy Protection Law coming into force in August 2025, ensure that there is a clear division of responsibilities between the Data Security Officer for the Ministry's databases and the appointed Privacy Supervisor, and monitor the execution of their respective roles.

- The Head of the Applications and Technology Department should instruct the heads of the departments and units in the Ministry of Defense to carry out a comprehensive mapping of all personal data in their possession, not only of the data transferred from the Ministry of Defense to external entities or received from them. He should also ensure that the mapping addresses the Privacy Protection Regulations (Instructions for Data that was Transferred to Israel from the European Economic Area), 2023. Following this, the Head of the Applications and Technology Department should identify the requirements applicable to the Ministry of Defense based on the mapping's findings, including the obligation to register such databases in the Database Public Registry.

- The Applications and Technology Department should periodically review all existing authorizations in the database systems connected to the Ministry of Defense's databases, including the Shemesh system, which is connected to the Disabled IDF Veterans Database, and revoke active authorizations that are not necessary for users to perform their duties. In addition, it is recommended that the Department also examine the

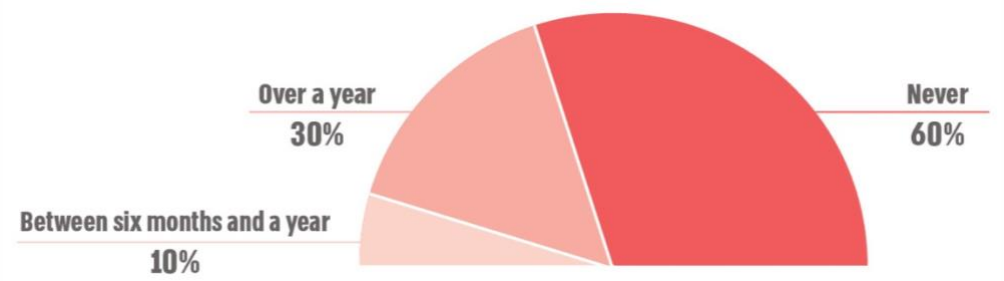
authorization management processes in the database systems. This will help reduce the risk of exposing personal data, including particularly sensitive information, to unauthorized individuals, as well as the risk that such data will be leaked, rendered unavailable or tampered with. In this way, the risk of harm to the privacy of individuals whose personal data is stored in the databases will be reduced.

- It is recommended that the Director General of the Ministry of Defense will regulate the division of responsibilities and authorities regarding data security under the Privacy Protection Law and the Data Security Regulations. This may be done, for example, by appointing a single entity with overall responsibility and a comprehensive view of all aspects of data security, including privacy protection considerations; by establishing an inter-department team to strengthen data security, comprising, for example, representatives from the Security Department, the Applications and Technology Department, the Office of the Legal Advisor to the Defense Establishment, and departments that use the databases; or by any other means deemed appropriate. It is further recommended that the division of responsibilities, authorities, and various roles, including with reference to Amendment No. 13 to the Privacy Protection Law, be anchored in a ministry procedure.

## The Potential Risk of External Users with Unnecessary Access Authorizations to a Central Computer Network of the Ministry of Defense

### The Percentage of External Users who have not Logged in to the Network for more than Six Months of all External Users with Active Network Access Permission


### Distribution of the Last Login Date of External Users who have not Logged in to the Network for more than Six Months




According to data from the Applications and Technology Department, processed by the State Comptroller's Office.

Given that this network serves as the gateway to the Ministry's databases, hosts assets – some of them sensitive – and supports the IDF's business operations and procurement processes, the risk of exposing sensitive information to unauthorized parties is increased, especially since 90% of the external users who have not logged in to the network for more than six months are outsourced workers.

# Summary

The Ministry of Defense controls databases containing personal data, such as data on a person's personality traits, health condition, and financial status. The risks to privacy and data security in these databases have increased, in light of the Swords of Iron War, and their materialization could impair the Ministry's ability to provide the Israel Defense Forces with the required resources, could cause reputational damage, harm relations with suppliers and customers, and expose it to fines. Moreover, such risks could sow panic and a sense of insecurity among the public, and damage the state's foreign relations in security and diplomatic contexts.

In recent years, data has leaked from the Ministry of Defense – both as a result of cyberattacks by hostile external actors and due to human error on the part of Ministry employees, including identifiable data about Ministry of Defense personnel.

The situation described in this report indicates serious gaps in the way the Ministry of Defense manages and secures the 14 databases under its control, which contain personal data on 2.84 million individuals. The audit found that the Applications and Technology Department, which is responsible for ensuring that the Ministry of Defense complies with the requirements imposed under the Privacy Protection Law and the Privacy Protection Regulations (Data Security), has not mapped all the databases controlled by the Ministry of Defense since 2007; has not established a data security procedure for the databases; has not conducted risk assessment surveys to identify data security risks in the databases that are classified as high security level; and has not performed penetration tests to the systems of these databases to assess their resilience against internal and external threats.

In addition, the report identified shortcomings in the management of user authorizations in the identity management system and in the database system linked to the IDF Disabled Veterans Database – a database containing data on approximately 230,000 individuals, including approximately 18,000 wounded persons added to the data as a result of the Swords of Iron War, with details on their health condition, financial status, family members, and the services provided to them. An analysis conducted by the State Comptroller's Office found that 5 out of 10 external users (outsourced employees) with active access permission to the database system linked to the IDF Disabled Veterans Database had not logged into it for more than six months. Furthermore, consultants managed in the Ministry of Defense's human resources systems, in the same way as ministry employees, had also not accessed the system for more than six months; their share of all users who had not logged in during that period was 20%. This situation raises concerns that they hold access authorizations to the IDF Disabled Veterans Database without necessity.

The Ministry of Defense should comply with the privacy protection requirements applicable to it under the Law and Regulations, particularly in light of Amendment No. 13 to the Law, which will enter into force in August 2025 and adapt the Law to current challenges. In addition, given the findings from the data analysis conducted by the State Comptroller's Office, it is

recommended that the Ministry examine its authorization management processes across all database systems connected to the Ministry's databases. It is further recommended that the Director General of the Ministry of Defense regulate the division of responsibilities and authorities between the Applications and Technology Department and the Security Department regarding data security from a privacy protection perspective. This will help to reduce the risks of privacy violations and of impairing the Ministry of Defense's ability to fulfill its mission.