SDAIA
الهيئة السعودية للبيانات والذكاء الاصطناعي
Saudi Data & AI Authority

مشروع قواعد تعيين مسؤول حماية البيانات الشخصية

Draft Rules for Appointing Personal Data Protection Officer

Table of Contents

الفهرس

المقدمة

أصدرت الهيئة السعودية للبيانات والذكاء الاصطناعي هذه القواعد استناداً إلى الفقرة (2) من المادة الثلاثون من نظام حماية البيانات الشخصية الصادر بالمرسوم الملكي رقم (م/19) وتاريخ 1443/2/9هـ والمعدل بموجب المرسوم الملكي رقم (م/148) وتاريخ 1444/9/5هـ والفقرة (4) من المادة الثانية والثلاثون من اللائحة التنفيذية للنظام.

Introduction

Saudi Data & AI Authority “SDAIA” issued these Rules based on Paragraph (2) of Article (30) of Personal Data Protection Law issued pursuant to Royal Decree No. (M/19) dated 09/02/1443 AH and amended pursuant to Royal Decree No. (M/148) dated 05/09/1444 AH, and Paragraph (4) of Article (32) of the Implementing Regulations of the Law.

المادة الأولى: التعريفات

-1 يُقصد بالألفاظ والعبارات الواردة في هذه القواعد المعاني المبينة لها أمام كل منها في المادة الأولى من نظام حماية البيانات الشخصية - ويشار إليه فيما بما يلي بـ "النظام"- الصادر بالمرسوم الملكي رقم (م/19) وتاريخ 1443/2/9هـ والمعدل بموجب المرسوم الملكي رقم (م/148) وتاريخ 1444/9/5هـ، والمادة الأولى من اللائحة التنفيذية لنظام حماية البيانات الشخصية ما لم يرد لها تعريف خاص في هذه القواعد.

-2 يُقصد بالألفاظ والعبارات الآتية -أينما وردت في هذه القواعد - المعاني المبينة أمام كل منها، ما لم يقتضِ السياق خلاف ذلك:

الجهة المختصة: الهيئة السعودية للبيانات والذكاء الاصطناعي

جهة التحكم: أي جهة عامة، وأي شخصية ذات صفة طبيعية أو اعتبارية خاصة؛ تحدد الغرض من معالجة البيانات الشخصية وكيفية ذلك؛ سواء أباشرت معالجة البيانات الشخصية بوساطتها أم بوساطة جهة المعالجة.

مسؤول حماية البيانات الشخصية: أي شخص طبيعي يتم تعيينه من قبل جهة التحكم يكون مسؤولا عن حماية البيانات الشخصية، ومراقبة الاجراءات المعمول بها داخل جهة التحكم والإشراف عليها لضمان التزامها بأحكام النظام ولوائحه، وتلقي الطلبات المتعلقة بالبيانات الشخصية وفقًا لأحكام النظام ولوائحه.

Article 1:Definitions

1. The terms and phrases mentioned herein shall have the meanings ascribed thereto in Article (1) of Personal Data Protection Law, hereinafter referred to as the "Law", issued pursuant to Royal Decree No. (M/19) dated 09/02/1443 AH and amended pursuant to Royal Decree No. (M/148) dated 05/09/1444 AH and Article (1) of the Implementing Regulations of the Law, unless they have a specific definition herein.

2. The following terms and phrases, wherever mentioned herein, shall have the meanings ascribed thereto, unless the context requires otherwise:

Competent Authority: Saudi Data & AI Authority (**SDAIA**).

Controller: Any Public Entity, natural person or private legal person that specifies the purpose and manner of Processing Personal Data, whether the data is processed by that Controller or by the Processor.

Data Protection Officer (DPO): Any individual appointed by Controller to be responsible for protecting Personal Data, monitoring and overseeing procedures applicable by Controller to ensure compliance with the provisions of the Law and its Regulations, and receiving requests related to Personal Data in accordance with provisions of the Law and its Regulations.

Article 2:Purpose

These Rules aim at:

1. Setting minimum requirements for appointing DPO.
2. Clarification of concepts related to cases in which Controller shall appoint DPO.

المادة الثانية: الغرض

تهدف هذه القواعد إلى الآتي:

1- وضع الحد الأدنى من متطلبات تعيين مسؤول حماية البيانات الشخصية.

2- ايضاح المفاهيم المتعلقة بالأحوال التي يجب فيها على جهة التحكم تعيين مسؤول حماية البيانات الشخصية.

Article 3:Scope of Application

These Rules shall apply to all Controllers covered by provisions of the Law and its Implementing Regulations.

المادة الثالثة: النطاق

تطبق هذه القواعد على جميع جهات التحكم المشمولة بتطبيق أحكام نظام حماية البيانات الشخصية ولوائحه التنفيذية.

Article 4:Requirements for DPO Appointment

1. When appointing DPO, Controller shall ensure that the following requirements are met:
   A. Having appropriate academic qualifications and experience in the field of Personal Data protection.
   B. Controller's business and activities that involve processing of Personal Data.
   C. Having sufficient knowledge of Personal Data breach risks.
   D. Having sufficient knowledge of regulatory measures for Personal Data protection and other relevant organizational measures for performing DPO tasks.
   E. Honesty and integrity, and not having been convicted of any offense involving dishonesty or breach of trust.
2. DPO may be an executive, employee of Controller or an external contractor.
3. The Competent Authority shall be entitled to request replacement of DPO if it is found that DPO is not competent.

المادة الرابعة: متطلبات تعيين مسؤول حماية البيانات الشخصية

1. يجب على جهة التحكم عند تعيين مسؤول حماية البيانات الشخصية أن تتأكد من توافر المتطلبات الآتية:

أ- توفر المؤهل العلمي المناسب والخبرة في مجال حماية البيانات الشخصية.

ب- معرفة كافية بالأعمال والأنشطة التي تتضمن معالجة بيانات شخصية لدى جهة التحكم.

ج- معرفة كافية بمعالجة مخاطر تسرب البيانات الشخصية.

د- معرفة كافية بالمتطلبات النظامية لحماية البيانات الشخصية والتنظيمية الأخرى ذات الصلة للقيام بمهام مسؤول حماية البيانات الشخصية.

ه- الأمانة والنزاهة وألا يكون قد أدين بأي جريمة مخلة بالشرف والأمانة.

2. يجوز أن يكون مسؤول حماية البيانات الشخصية مسؤولًا أو موظفًا لدى جهة التحكم أو متعاقدًا خارجيًا.

3. يجوز للجهة المختصة طلب استبدال مسؤول حماية البيانات الشخصية في حال تبين لها عدم كفاءته.

Article 5: Cases of Appointing DPO

First: Controller shall appoint one or more individuals to be responsible for protection of Personal Data in any of the following cases:

1. Controller is a Public Entity that provides services involving Processing of Personal Data on a large scale.
2. Controller core activities are based on processing operations that, by their nature, require regular and systematic monitoring of Data Subjects.
3. Core activities of Controller are based on processing of sensitive Personal Data.

Second: The term "processing of Personal Data on a large scale" refers to:

1. Processing operations that target a large group of Data Subjects.
2. Processing operations that aim to process a considerable amount of Personal Data.
3. Processing a wide variety of categories of Personal Data Subjects.

Third: The term “regular and systematic monitoring of Data Subjects” refers to:

Continuous processing by monitoring, tracking and profiling Data Subjects with the aim of improving or marketing services and products. **Activities that support Controller core activities shall not be considered core activities, such as processing job applications, payroll and other support activities at Controller.**

المادة الخامسة: أحوال تعيين مسؤول حماية البيانات الشخصية

أولاً: يجب على جهة التحكم تعيين أو تحديد شـــخصًـــا أو أكثر ليكون مسؤولا عن حماية البيانات الشخصية في أي من الأحوال الآتية:

1. في حال كانت جهة التحكم جهة عامة تقدم خدمات تتضـــمن معالجة بيانات شخصية على نطاق واسع.
2. أن تقوم الأنشطة الأساسية لجهة التحكم على عمليات المعالجة التي تتطلب بطبيعتها مراقبة منتظمة وممنهجة لأصـــحاب البيانات الشخصية.
3. أن تقوم الأنشـطة الأســاســية لجهة التحكم على معالجة بيانات حساسة.

ثانياً: المقصود بمعالجة البيانات الشخصية على نطاق واسع:

1. عمليات المعالجة التي تســتهدف مجموعة كبيرة من أصـــحاب البيانات الشخصية.
2. عمليات المعالجة التي تســتهدف مجموعة ضـــخمة من البيانات الشخصية.
3. معالجة مجموعة مختلفة من فئات أصحاب البيانات الشخصية.

ثالثاً: المقصـــود بالمراقبة المنتظمة والممنهجة لأصـــحاب البيانات الشخصية:

معالجة مستمرة من خلال مراقبة وتتبع وتنميط أصحاب البيانات الشخصية بهدف تحسين أو تسويق الخدمات والمنتجات.

ولا تشـكل الأنشـطة التي تدعم الأعمال الرئيسـية لجهة التحكم أنشـطة أساسية؛ مثل معالجة طلبات التوظيف ودفع الرواتب وغيرها من الأنشطة الداعمة داخل جهة التحكم.

Article 6:Documenting DPO Appointment

1. DPO shall be appointed in writing, by documenting DPO appointment in case DPO is an employee of Controller or an external contractor.

2. DPO appointment and means of communication with DPO shall be immediately announced within Controller.

المادة السادسة: توثيق تعيين مسؤول حماية البيانات الشخصية

1. يجب تعيين مسؤول حماية البيانات الشخصية كتابياً من خلال توثيق تعيين مسؤول حماية البيانات الشخصية في حال كان موظف لدى جهة التحكم أو متعاقداً خارجياً.

2. يجب أن يتم الإعلان فوراً داخل جهة التحكم عن تعيين مسؤول حماية البيانات الشخصية ووسيلة التواصل معه.

Article 7: DPO Contact Details

1. Controller shall make DPO contact details, i.e. e-mail and phone number, available in a clear and accessible manner in Privacy Policy to Data Subjects.

2. Controller shall immediately provide Competent Authority with contact details of DPO upon their appointment through the National Data Governance Platform, provided that such details include name and contact details, including e-mail and phone number.

المادة السابعة: تفاصيل الاتصال بمسؤول حماية البيانات الشخصية

1. على جهة التحكم إتاحة بيانات التواصل الخاصة بمسؤول حماية البيانات الشخصية لأصحاب البيانات الشخصية – عنوان البريد الإلكتروني ورقم الهاتف - بصورة واضحة ومتاحة في سياسة الخصوصية.

2. على جهة التحكم تزويد الجهة المختصة ببيانات التواصل مع مسؤول حماية البيانات الشخصية على الفور عند تعيينه، وذلك من خلال منصة حوكمة البيانات الوطنية، على أن تتضمن هذه التفاصيل الاسم وتفاصيل الاتصال به، بما في ذلك عنوان البريد الإلكتروني ورقم الهاتف.

Article 8: DPO Roles & Tasks

DPO shall be responsible for performing tasks stated in Paragraph (3) of Article (32) of the Implementing Regulations of the Law, in addition to the following tasks:

1. Providing support and advice regarding all aspects of Personal Data protection, including contributing to developing policies and internal procedures related to Personal Data protection at Controller.

2. Participating in awareness activities, training and transfer of knowledge to Controller personnel regarding Personal Data protection and compliance with provisions of the Law, Regulations and ethics of data handling.

3. Contributing to reviewing plans of response to Personal Data Breach incidents, and ensuring that such plans are adequate and effective.

المادة الثامنة: أدوار ومهام مسؤول حماية البيانات الشخصية

على مسؤول حماية البيانات الشخصية القيام بالمهام المشار إليها في الفقرة رقم (3) من المادة الثانية والثلاثون من اللائحة التنفيذية للنظام، بالإضافة إلى المهام الآتية:

1. تقديم الدعم والمشورة فيما يتعلق بجميع جوانب حماية البيانات الشخصية بما في ذلك المساهمة في تطوير السياسات والإجراءات الداخلية المتعلقة بحماية البيانات الشخصية داخل جهة التحكم.

2. المشاركة في الأنشطة التوعوية وتدريب ونقل المعرفة لمنسوبي جهة التحكم فيما يتعلق بحماية البيانات الشخصية والالتزام بأحكام النظام واللوائح وأخلاقيات التعامل مع البيانات.

3. المساهمة في مراجعة خطط الاستجابة لحوادث تسرب البيانات الشخصية والتأكد من مناسبتها وفعاليتها.

4. Preparing periodic reports regarding Controller activities related to processing of Personal Data, and providing recommendations to ensure compliance with provisions of the Law and its Regulations.

5. Maintaining the confidentiality of Personal Data and its level of sensitivity, based on its classification and relevant regulatory requirements to determine the adequate level of protection and processing mechanism.

6. Monitoring the Competent Authority's issued laws, regulations and instructions and the equivalent, implementing any amendments thereto and informing the relevant departments of the same to ensure compliance therewith.

7. Collaborating with individuals responsible for implementing activities related to AI ethics to ensure that the requirements of Personal Data protection and Data Subjects' privacy are met.

Article 9: General Provisions

1. Controllers shall periodically review DPO appointment cases to determine whether such cases are still required or likely to become mandatory according to provisions hereof.

2. When making an agreement between Controller and Processor for the purpose of processing of Personal Data for and on behalf of Controller, Controller shall ensure that Processor has DPO or request appointment of DPO in cases that require appointing DPO with the aim of ensuring application of appropriate safeguards for implementing provisions of the Law and Regulations.

3. When appointing DPO, Controller shall not assign tasks that may conflict with DPO tasks or affect DPO's independence.

4. The Controller shall work on training and developing DPO's in the fields of Personal Data protection and support them in obtaining professional certificates in this field to ensure raising their efficiency.

4. إعداد تقارير دورية حيال أنشـــطة جهة التحكم المتعلقة بمعالجة البيانات الشخصية وتقديم التوصيات بشأنها لضمان الالتزام بأحكام النظام ولوائحه.

5. المحافظة على سرية البيانات الشخصية ودرجة حساسيتها بحسب مســـتوى تصـــنيفها ووفقاً للمتطلبات التنظيمية ذات العلاقة، وذلك لتحديد مستوى الحماية المناسب لها وآلية معالجتها.

6. متابعة ما يصـدر عن الجهة المختصـة من أنظمة ولوائح وتعليمات وما في حكمها وأي تعديلات تجرى عليها وإحاطة الإدارات ذات العلاقة بذلك لضمان الالتزام بها.

7. المشـاركة مع الأشـخاص المسـؤولين عن تنفيذ الأنشـطة المتعلقة بأخلاقيات الذكاء الاصطناعي لضمان توفر متطلبات حماية البيانات الشخصية وخصوصية أصحابها.

المادة التاسعة: أحكام عامة

1. يجب على جهات التحكم مراجعة أحوال تعيين مســؤول حماية البيانات الشخصية بشكل دوري وما إذا كان لا يزال أو من المحتمل أن يصبح إلزامياً وفقاً لأحكام هذه القواعد.

2. عند إبرام اتفاقية بين جهة التحكم وجهة المعالجة بغرض معالجة البيانات الشخصية لمصلحة جهة التحكم ونيابةً عنها، لجهة التحكم التحقق من توافر مسؤول حماية بيانات شخصية لدى جهة المعالجة أو طلب تعيينه في الحالات التي تتطلب تعيين مســؤول حماية البيانات الشخصية وذلك بهدف التأكد من توفر الضمانات اللازمة لتنفيذ أحكام النظام واللوائح.

3. يجب على جهة التحكم عند تعيين مسؤول حماية البيانات الشخصية عدم تكليفه بمهام قد تتعارض مع مهامه كمســؤول حماية البيانات الشخصية أو تؤثر على استقلاليته.

4. يجب على جهة التحكم العمل على تدريب وتطوير مسؤولي حماية البيانات الشخصية في مجالات حماية البيانات الشخصية ودعمهم في الحصـــول على شـــهادات مهنية في هذا المجال لضـــمان رفع كفاءتهم.

Article 10:Review and Amendment

The Competent Authority shall review these Rules when required, and may introduce any amendment or update thereto.

المادة العاشرة: المراجعة والتعديل

تقوم الجهة المختصـة بمراجعة هذه القواعد - عند الاقتضـاء- ولها اجراء أي تعديل أو تحديث عليها.

Article 11:Entry Into Force

These Rules shall come into force as of the date of publishing on the Competent Authority's official website.

المادة الحادية عشرة: النفاذ

يُعمل بهذه القواعد اعتباراً من تاريخ النشـــر في موقع الجهة المختصـــة الرسمي.