Mandatory Review of Personal Data Handling Policy Paper

August 2026

Personal Data Policy Institute

Note: This document is fictitious material made up for training and practice. It is not a real law or government publication.

Contents

Chapter 1 General provisions and obligations 3
Chapter 2 Background to the scheme 20
Chapter 3 Results of the domestic survey 39
Chapter 4 Overseas cases 45
Chapter 5 Support for compliance 61
Chapter 6 Supervision and sanctions 71
Addenda 77
Annex tables · forms 80

Notes on this paper

This paper sets out the mandatory review of personal data handling as articles and commentary. The articles are in Chapters 1 and 6; background and reference material are in Chapters 2 to 5.

Chapter 1 General provisions and obligations

Section 1 Overview

This chapter holds the framework of the mandatory review of personal data handling. It first states when the scheme starts and whom it covers, then sets out as articles the obligations a business must meet.

The aim of the scheme is simple: whoever handles personal data should look at their own handling regularly and leave a record of having done so. Behind it lies the judgement that investigating after an incident is too late.

Chapter 1 is organised as follows. Section 1 is the overview, Section 2 covers definitions and scope, and Section 3 the obligations of businesses. Matters of commencement are placed separately in the Addenda, and their gist is copied on the next page.

Section 2 Commencement

Addenda, Article 1 (Date of commencement)

This scheme takes effect on 1 January 2027.

The date of commencement was set with regard to the time needed to prepare after promulgation. Personal data handling carried out before that date is governed by the previous standards.

The first review cycle after commencement is counted from the year in which the date of commencement falls. A review completed within six months after commencement, however, counts as that year's review.

Details on the date of commencement are covered again in Chapter 6 and the Addenda.

Addenda, Article 2 (Deferred application)

> For businesses with fewer than 50 permanent employees, application of this scheme is deferred for one year from the date of commencement.

Whether a business qualifies for deferral is judged as at the last day of the month in which the date of commencement falls. If a business reaches 50 or more permanent employees during the deferral, the scheme applies from the year after the year in which that happened.

The method of counting permanent employees follows Annex Table 1, which also decides whether dispatched and part-time workers are counted.

Even a business with deferral is not exempt from the breach notification and reporting duty in Article 9. This point is often misunderstood in practice.

Section 3 Definitions

Article 2 (Definitions) The terms used in this paper mean the following.

1. "Personal data" means information about a living individual by which that individual can be identified.

2. "Handling" means collecting, generating, recording, storing, holding, processing, editing, searching, outputting, correcting, restoring, using, providing, disclosing or destroying personal data, and any similar act.

3. "Handling status" means the facts of which personal data is held, for what purpose, where, and who deals with it.

4. "Review" means the series of acts of examining the handling status, confirming whether it meets the standards, and recording the result.

5. "Processor" means a person entrusted with handling personal data on another's behalf.

Section 4 Scope

Article 3 (Scope of application)

This scheme applies to every business that handles personal data, regardless of industry, size or volume of personal data handled.

Only a business that handles no personal data at all is outside its scope. Since handling the HR and payroll data of staff already counts as handling personal data, a business that is actually not covered is rare.

Public bodies follow separate guidelines and are not dealt with in this paper.

Even within scope, the date of application may differ by size. Read this together with the deferral in Article 2 of the Addenda.

Section 5 Relation to other standards

Article 4 (Relation to other standards) Where another standard has a special provision on personal data protection, that standard applies.

This scheme does not replace existing personal data protection duties. It is more accurate to see it as a procedure of "checking regularly and leaving a record" placed on top of the existing duties.

A business already certified under an information security management system may substitute the review in Article 7 within the range confirmed in its certification audit. The range of substitution is set in Annex Table 2.

Article 5 (Duty of businesses)

When handling personal data, a business must make sure the rights of data subjects are not infringed. To that end it must understand and manage its own handling status.

Article 6 (Appointment of a responsible person)

A business must appoint a person responsible for overseeing personal data handling. That person leads the review under Article 7 and reports its result to the head of the business.

In a small business where a separate responsible person is hard to appoint, the head of the business may take that role.

Article 6-2 (Basic plan)

The competent policy authority draws up a basic plan for the review of personal data handling every three years. The basic plan covers the following.

1. Improving the review standards
2. Support for businesses
3. Timing and method of the survey
4. Other matters needed to run the scheme

The content of the basic plan and its progress are published every year.

Section 6 Obligations of businesses

This section sets the obligations a business must meet. There are three: regular review of handling with record keeping, required contents in outsourcing contracts, and notification and reporting of a breach.

The three obligations are independent of each other. Meeting one does not exempt a business from another. The article for each obligation follows from the next page.

Compliance is confirmed through records. Note that where a business complied but has no record, it will find it hard to prove compliance during supervision.

Article 7 (Review of handling status and keeping of records)

(1) A business must review its personal data handling status at least once a year.

(2) A business must record the result of the review and keep that record for three years.

(3) The business decides when to review. Once set, however, the timing is not changed without a special reason.

(4) Where the review finds a matter that does not meet the standards, the matter and the action taken must be recorded together.

This article is the core of the scheme. What is required is not the fact of having reviewed, but a record of what was looked at, how, and what was found.

Commentary on Article 7 — Review items

The items to confirm in a review are as follows. The detailed form is in Annex Table 3.

1. Types and items of personal data collected
2. Purpose of collection and retention period
3. Storage location and who has access
4. Provision to third parties and outsourcing
5. Whether personal data past its retention period has been destroyed
6. State of access log keeping

For each item write "confirmed / could not confirm / not applicable", and for any item not confirmed write the reason.

Commentary on Article 7 — How to record

The form of the record is not prescribed. Paper or an electronic file are both acceptable. The following four, however, must be shown.

Date of review · Reviewer · Scope of review · Matters found and action taken

Where the review was limited to part of the scope, state what was excluded. A record that does not state its scope may not be accepted as a record of compliance.

The three-year retention of the record runs from the day the review was completed.

Article 8 (Required contents of an outsourcing contract)

When a business outsources the handling of personal data, the contract must state the following five items.

1. Purpose and scope of the outsourced work
2. Restrictions on sub-outsourcing
3. Measures to ensure the security of personal data
4. Management and supervision of the processor
5. Liability, including compensation for damage

A contract missing even one of the five items is regarded as breaching this article. The same applies where the wording is too vague to impose the duty.

Commentary on Article 8 — Managing and supervising the processor

Management and supervision do not end with writing them into the contract. The business must actually confirm that the processor handles personal data securely.

The frequency and method of confirmation are set in the contract. Where they are not set, it is hard to regard confirmation as made at least once a year.

The result of the confirmation may be kept as part of the review record under Article 7.

Commentary on Article 8 — Sub-outsourcing

A processor that wants to pass the outsourced work to someone else needs the consent of the business. Even if the contract says nothing on this, sub-outsourcing without consent is not allowed.

Consent is to be obtained in writing as a rule. An electronic document counts as writing.

Where sub-outsourcing takes place, the business's duty of management and supervision extends to the sub-processor.

Commentary on Article 8 — On termination of the contract

When the outsourcing contract ends, the processor must destroy the personal data it holds or return it to the business. Which of the two applies is set in the contract in advance.

Where the data is destroyed, the processor informs the business and keeps evidence. The evidence includes the date, scope and method of destruction.

Where the data must be kept for some time after the contract ends, the contract must state the grounds and the period.

Article 9 (Notification and reporting of a breach)

(1) A business that becomes aware that personal data has been leaked must notify the data subjects without delay.

(2) The business must report to the competent authority within 72 hours of becoming aware of the breach.

(3) Where there is a reason it is hard to report within 72 hours, the business may report first with that reason and supplement the confirmed facts later.

(4) The duty to report is not waived even where the breach is small.

This duty also applies to businesses that have deferral under Article 2 of the Addenda.

Chapter 2 Background to the scheme

Ch.2 Sec.1

We look first at the situation before the scheme. Rules on personal data protection have existed for a long time, but there was no procedure that made a business check for itself whether it was following them.

What was commonly observed in practice was this: personal data no one used stayed on file for years, leavers kept their access rights, and outsourcing contracts were still on a form from several years earlier.

What was needed, then, was not a new prohibition but a mechanism that makes businesses look regularly. That judgement is the starting point of this scheme.

Ch.2 Sec.2

As a result, supervision happened only after an incident. What had been wrong before the incident came to light only during the investigation.

This state of affairs did not come from an intention to break the rules. Most of it arose because something set up once was never looked at again.

The next sections look in turn at the material on which that judgement rests.

Ch.2 Sec.3

What was commonly observed in practice was this: personal data no one used stayed on file for years, leavers kept their access rights, and outsourcing contracts were still on a form from several years earlier.

What was needed, then, was not a new prohibition but a mechanism that makes businesses look regularly. That judgement is the starting point of this scheme.

We look first at the situation before the scheme. Rules on personal data protection have existed for a long time, but there was no procedure that made a business check for itself whether it was following them.

Ch.2 Sec.4

This state of affairs did not come from an intention to break the rules. Most of it arose because something set up once was never looked at again.

The next sections look in turn at the material on which that judgement rests.

As a result, supervision happened only after an incident. What had been wrong before the incident came to light only during the investigation.

Ch.2 Sec.5

What was needed, then, was not a new prohibition but a mechanism that makes businesses look regularly. That judgement is the starting point of this scheme.

We look first at the situation before the scheme. Rules on personal data protection have existed for a long time, but there was no procedure that made a business check for itself whether it was following them.

What was commonly observed in practice was this: personal data no one used stayed on file for years, leavers kept their access rights, and outsourcing contracts were still on a form from several years earlier.

Ch.2 Sec.6

The next sections look in turn at the material on which that judgement rests.

As a result, supervision happened only after an incident. What had been wrong before the incident came to light only during the investigation.

This state of affairs did not come from an intention to break the rules. Most of it arose because something set up once was never looked at again.

Ch.2 Sec.7

We look first at the situation before the scheme. Rules on personal data protection have existed for a long time, but there was no procedure that made a business check for itself whether it was following them.

What was commonly observed in practice was this: personal data no one used stayed on file for years, leavers kept their access rights, and outsourcing contracts were still on a form from several years earlier.

What was needed, then, was not a new prohibition but a mechanism that makes businesses look regularly. That judgement is the starting point of this scheme.

Ch.2 Sec.8

As a result, supervision happened only after an incident. What had been wrong before the incident came to light only during the investigation.

This state of affairs did not come from an intention to break the rules. Most of it arose because something set up once was never looked at again.

The next sections look in turn at the material on which that judgement rests.

Ch.2 Sec.9

What was commonly observed in practice was this: personal data no one used stayed on file for years, leavers kept their access rights, and outsourcing contracts were still on a form from several years earlier.

What was needed, then, was not a new prohibition but a mechanism that makes businesses look regularly. That judgement is the starting point of this scheme.

We look first at the situation before the scheme. Rules on personal data protection have existed for a long time, but there was no procedure that made a business check for itself whether it was following them.

Ch.2 Sec.10

This state of affairs did not come from an intention to break the rules. Most of it arose because something set up once was never looked at again.

The next sections look in turn at the material on which that judgement rests.

As a result, supervision happened only after an incident. What had been wrong before the incident came to light only during the investigation.

Ch.2 Sec.11

What was needed, then, was not a new prohibition but a mechanism that makes businesses look regularly. That judgement is the starting point of this scheme.

We look first at the situation before the scheme. Rules on personal data protection have existed for a long time, but there was no procedure that made a business check for itself whether it was following them.

What was commonly observed in practice was this: personal data no one used stayed on file for years, leavers kept their access rights, and outsourcing contracts were still on a form from several years earlier.

Ch.2 Sec.12

The next sections look in turn at the material on which that judgement rests.

As a result, supervision happened only after an incident. What had been wrong before the incident came to light only during the investigation.

This state of affairs did not come from an intention to break the rules. Most of it arose because something set up once was never looked at again.

Ch.2 Sec.13

We look first at the situation before the scheme. Rules on personal data protection have existed for a long time, but there was no procedure that made a business check for itself whether it was following them.

What was commonly observed in practice was this: personal data no one used stayed on file for years, leavers kept their access rights, and outsourcing contracts were still on a form from several years earlier.

What was needed, then, was not a new prohibition but a mechanism that makes businesses look regularly. That judgement is the starting point of this scheme.

Ch.2 Sec.14

As a result, supervision happened only after an incident. What had been wrong before the incident came to light only during the investigation.

This state of affairs did not come from an intention to break the rules. Most of it arose because something set up once was never looked at again.

The next sections look in turn at the material on which that judgement rests.

Ch.2 Sec.15

What was commonly observed in practice was this: personal data no one used stayed on file for years, leavers kept their access rights, and outsourcing contracts were still on a form from several years earlier.

What was needed, then, was not a new prohibition but a mechanism that makes businesses look regularly. That judgement is the starting point of this scheme.

We look first at the situation before the scheme. Rules on personal data protection have existed for a long time, but there was no procedure that made a business check for itself whether it was following them.

Ch.2 Sec.16

This state of affairs did not come from an intention to break the rules. Most of it arose because something set up once was never looked at again.

The next sections look in turn at the material on which that judgement rests.

As a result, supervision happened only after an incident. What had been wrong before the incident came to light only during the investigation.

Ch.2 Sec.17

What was needed, then, was not a new prohibition but a mechanism that makes businesses look regularly. That judgement is the starting point of this scheme.

We look first at the situation before the scheme. Rules on personal data protection have existed for a long time, but there was no procedure that made a business check for itself whether it was following them.

What was commonly observed in practice was this: personal data no one used stayed on file for years, leavers kept their access rights, and outsourcing contracts were still on a form from several years earlier.

Ch.2 Sec.18

The next sections look in turn at the material on which that judgement rests.

As a result, supervision happened only after an incident. What had been wrong before the incident came to light only during the investigation.

This state of affairs did not come from an intention to break the rules. Most of it arose because something set up once was never looked at again.

Ch.2 Sec.19

We look first at the situation before the scheme. Rules on personal data protection have existed for a long time, but there was no procedure that made a business check for itself whether it was following them.

What was commonly observed in practice was this: personal data no one used stayed on file for years, leavers kept their access rights, and outsourcing contracts were still on a form from several years earlier.

What was needed, then, was not a new prohibition but a mechanism that makes businesses look regularly. That judgement is the starting point of this scheme.

Chapter 3 Results of the domestic survey

Ch.3 Sec.1

The survey was carried out in the second half of 2025. The sample was drawn by industry and size, and both a questionnaire and on-site checks were used.

The survey found that many of the responding businesses had no complete list of the personal data their own organisation holds.

The smaller the business, the clearer this tendency. A large business, however, was not necessarily thorough either.

Ch.3 Sec.2

The survey found that many of the responding businesses had no complete list of the personal data their own organisation holds.

Even among businesses that had outsourcing contracts, fewer than half had a clause on security measures in the contract.

The survey was carried out in the second half of 2025. The sample was drawn by industry and size, and both a questionnaire and on-site checks were used.

Ch.3 Sec.3

Even among businesses that had outsourcing contracts, fewer than half had a clause on security measures in the contract.

The smaller the business, the clearer this tendency. A large business, however, was not necessarily thorough either.

The survey found that many of the responding businesses had no complete list of the personal data their own organisation holds.

Ch.3 Sec.4

The smaller the business, the clearer this tendency. A large business, however, was not necessarily thorough either.

The survey was carried out in the second half of 2025. The sample was drawn by industry and size, and both a questionnaire and on-site checks were used.

Even among businesses that had outsourcing contracts, fewer than half had a clause on security measures in the contract.

Ch.3 Sec.5

The survey was carried out in the second half of 2025. The sample was drawn by industry and size, and both a questionnaire and on-site checks were used.

The survey found that many of the responding businesses had no complete list of the personal data their own organisation holds.

The smaller the business, the clearer this tendency. A large business, however, was not necessarily thorough either.

Ch.3 Sec.6

The survey found that many of the responding businesses had no complete list of the personal data their own organisation holds.

Even among businesses that had outsourcing contracts, fewer than half had a clause on security measures in the contract.

The survey was carried out in the second half of 2025. The sample was drawn by industry and size, and both a questionnaire and on-site checks were used.

Chapter 4 Overseas cases

Ch.4 Sec.1

This chapter looks at similar schemes overseas. It is reference material and is not a basis for interpreting our scheme.

Listing the required contents of an outsourcing contract in law is also common. The number of items differs from country to country, but five strands are broadly shared: purpose and scope, security measures, sub-outsourcing, supervision and liability.

Many set the deadline for reporting a breach at 72 hours. Counting the deadline from "the time the business became aware" is also common.

Ch.4 Sec.2

Many countries require regular self-review and record keeping. The review cycle is usually one year; how long the record is kept differs by country.

Many set the deadline for reporting a breach at 72 hours. Counting the deadline from "the time the business became aware" is also common.

Approaches to sanctions differ. Some link the penalty to turnover, others use fixed bands, and both are in use.

Ch.4 Sec.3

Listing the required contents of an outsourcing contract in law is also common. The number of items differs from country to country, but five strands are broadly shared: purpose and scope, security measures, sub-outsourcing, supervision and liability.

Approaches to sanctions differ. Some link the penalty to turnover, others use fixed bands, and both are in use.

This chapter looks at similar schemes overseas. It is reference material and is not a basis for interpreting our scheme.

Ch.4 Sec.4

Many set the deadline for reporting a breach at 72 hours. Counting the deadline from "the time the business became aware" is also common.

This chapter looks at similar schemes overseas. It is reference material and is not a basis for interpreting our scheme.

Many countries require regular self-review and record keeping. The review cycle is usually one year; how long the record is kept differs by country.

Ch.4 Sec.5

Approaches to sanctions differ. Some link the penalty to turnover, others use fixed bands, and both are in use.

Many countries require regular self-review and record keeping. The review cycle is usually one year; how long the record is kept differs by country.

Listing the required contents of an outsourcing contract in law is also common. The number of items differs from country to country, but five strands are broadly shared: purpose and scope, security measures, sub-outsourcing, supervision and liability.

Ch.4 Sec.6

This chapter looks at similar schemes overseas. It is reference material and is not a basis for interpreting our scheme.

Listing the required contents of an outsourcing contract in law is also common. The number of items differs from country to country, but five strands are broadly shared: purpose and scope, security measures, sub-outsourcing, supervision and liability.

Many set the deadline for reporting a breach at 72 hours. Counting the deadline from "the time the business became aware" is also common.

Ch.4 Sec.7

Many countries require regular self-review and record keeping. The review cycle is usually one year; how long the record is kept differs by country.

Many set the deadline for reporting a breach at 72 hours. Counting the deadline from "the time the business became aware" is also common.

Approaches to sanctions differ. Some link the penalty to turnover, others use fixed bands, and both are in use.

Ch.4 Sec.8

Listing the required contents of an outsourcing contract in law is also common. The number of items differs from country to country, but five strands are broadly shared: purpose and scope, security measures, sub-outsourcing, supervision and liability.

Approaches to sanctions differ. Some link the penalty to turnover, others use fixed bands, and both are in use.

This chapter looks at similar schemes overseas. It is reference material and is not a basis for interpreting our scheme.

Ch.4 Sec.9

Many set the deadline for reporting a breach at 72 hours. Counting the deadline from "the time the business became aware" is also common.

This chapter looks at similar schemes overseas. It is reference material and is not a basis for interpreting our scheme.

Many countries require regular self-review and record keeping. The review cycle is usually one year; how long the record is kept differs by country.

Ch.4 Sec.10

Approaches to sanctions differ. Some link the penalty to turnover, others use fixed bands, and both are in use.

Many countries require regular self-review and record keeping. The review cycle is usually one year; how long the record is kept differs by country.

Listing the required contents of an outsourcing contract in law is also common. The number of items differs from country to country, but five strands are broadly shared: purpose and scope, security measures, sub-outsourcing, supervision and liability.

Ch.4 Sec.11

This chapter looks at similar schemes overseas. It is reference material and is not a basis for interpreting our scheme.

Listing the required contents of an outsourcing contract in law is also common. The number of items differs from country to country, but five strands are broadly shared: purpose and scope, security measures, sub-outsourcing, supervision and liability.

Many set the deadline for reporting a breach at 72 hours. Counting the deadline from "the time the business became aware" is also common.

Ch.4 Sec.12

Many countries require regular self-review and record keeping. The review cycle is usually one year; how long the record is kept differs by country.

Many set the deadline for reporting a breach at 72 hours. Counting the deadline from "the time the business became aware" is also common.

Approaches to sanctions differ. Some link the penalty to turnover, others use fixed bands, and both are in use.

Ch.4 Sec.13

Listing the required contents of an outsourcing contract in law is also common. The number of items differs from country to country, but five strands are broadly shared: purpose and scope, security measures, sub-outsourcing, supervision and liability.

Approaches to sanctions differ. Some link the penalty to turnover, others use fixed bands, and both are in use.

This chapter looks at similar schemes overseas. It is reference material and is not a basis for interpreting our scheme.

Ch.4 Sec.14

Many set the deadline for reporting a breach at 72 hours. Counting the deadline from "the time the business became aware" is also common.

This chapter looks at similar schemes overseas. It is reference material and is not a basis for interpreting our scheme.

Many countries require regular self-review and record keeping. The review cycle is usually one year; how long the record is kept differs by country.

Ch.4 Sec.15

Approaches to sanctions differ. Some link the penalty to turnover, others use fixed bands, and both are in use.

Many countries require regular self-review and record keeping. The review cycle is usually one year; how long the record is kept differs by country.

Listing the required contents of an outsourcing contract in law is also common. The number of items differs from country to country, but five strands are broadly shared: purpose and scope, security measures, sub-outsourcing, supervision and liability.

Ch.4 Sec.16

This chapter looks at similar schemes overseas. It is reference material and is not a basis for interpreting our scheme.

Listing the required contents of an outsourcing contract in law is also common. The number of items differs from country to country, but five strands are broadly shared: purpose and scope, security measures, sub-outsourcing, supervision and liability.

Many set the deadline for reporting a breach at 72 hours. Counting the deadline from "the time the business became aware" is also common.

Chapter 5 Support for compliance

Ch.5 Sec.1

This chapter sets out the measures to support compliance.

First, a review form and examples are distributed. The form in Annex Table 3 can be used as it is.

Second, a standard outsourcing contract is provided. Its wording includes all five items of Article 8.

Ch.5 Sec.2

First, a review form and examples are distributed. The form in Annex Table 3 can be used as it is.

Second, a standard outsourcing contract is provided. Its wording includes all five items of Article 8.

Third, an advice desk is set up for small businesses. What is discussed there is not used as supervision material.

Second, a standard outsourcing contract is provided. Its wording includes all five items of Article 8.

Third, an advice desk is set up for small businesses. What is discussed there is not used as supervision material.

Fourth, in the first year guidance comes before enforcement. The scope and period of guidance will be announced separately.

Ch.5 Sec.4

Third, an advice desk is set up for small businesses. What is discussed there is not used as supervision material.

Fourth, in the first year guidance comes before enforcement. The scope and period of guidance will be announced separately.

This chapter sets out the measures to support compliance.

Fourth, in the first year guidance comes before enforcement. The scope and period of guidance will be announced separately.

This chapter sets out the measures to support compliance.

First, a review form and examples are distributed. The form in Annex Table 3 can be used as it is.

Ch.5 Sec.6

This chapter sets out the measures to support compliance.

First, a review form and examples are distributed. The form in Annex Table 3 can be used as it is.

Second, a standard outsourcing contract is provided. Its wording includes all five items of Article 8.

Ch.5 Sec.7

First, a review form and examples are distributed. The form in Annex Table 3 can be used as it is.

Second, a standard outsourcing contract is provided. Its wording includes all five items of Article 8.

Third, an advice desk is set up for small businesses. What is discussed there is not used as supervision material.

Second, a standard outsourcing contract is provided. Its wording includes all five items of Article 8.

Third, an advice desk is set up for small businesses. What is discussed there is not used as supervision material.

Fourth, in the first year guidance comes before enforcement. The scope and period of guidance will be announced separately.

Ch.5 Sec.9

Third, an advice desk is set up for small businesses. What is discussed there is not used as supervision material.

Fourth, in the first year guidance comes before enforcement. The scope and period of guidance will be announced separately.

This chapter sets out the measures to support compliance.

Fourth, in the first year guidance comes before enforcement. The scope and period of guidance will be announced separately.

This chapter sets out the measures to support compliance.

First, a review form and examples are distributed. The form in Annex Table 3 can be used as it is.

Chapter 6 Supervision and sanctions

Article 33 (Administrative fines)

(1) An administrative fine is imposed on any person who falls under one of the following.

1. A person who fails to review, or fails to keep the record, in breach of Article 7

2. A person who leaves out a required item in breach of Article 8

3. A person who fails to report within the deadline in breach of Article 9

(2) The amount bands of the fine and the criteria for imposing it are set by enforcement decree.

(3) The fine is imposed and collected by the competent authority.

The fine may be reduced according to the degree and number of breaches and whether they were corrected. The grounds and limits of reduction are also set by enforcement decree.

Ch.6 Sec.2 Supervision procedure

Supervision is by written review as a rule. On-site checks are made only where necessary.

A business given a corrective order must comply within the set period and report the result.

A business that objects may contest the order through the set procedure.

Ch.6 Sec.3 Supervision procedure

A business given a corrective order must comply within the set period and report the result.

A business that objects may contest the order through the set procedure.

Supervision is by written review as a rule. On-site checks are made only where necessary.

Ch.6 Sec.4 Supervision procedure

A business that objects may contest the order through the set procedure.

Supervision is by written review as a rule. On-site checks are made only where necessary.

A business given a corrective order must comply within the set period and report the result.

Ch.6 Sec.5 Supervision procedure

Supervision is by written review as a rule. On-site checks are made only where necessary.

A business given a corrective order must comply within the set period and report the result.

A business that objects may contest the order through the set procedure.

Ch.6 Sec.6 Supervision procedure

A business given a corrective order must comply within the set period and report the result.

A business that objects may contest the order through the set procedure.

Supervision is by written review as a rule. On-site checks are made only where necessary.

Addenda

Article 1 (Date of commencement) This scheme takes effect on 1 January 2027.

Article 2 (Deferred application) For businesses with fewer than 50 permanent employees, application is deferred for one year from the date of commencement.

Article 3 (Transitional provision) An outsourcing contract already concluded when this scheme takes effect may follow the previous rules until its renewal date or one year after the date of commencement, whichever comes first.

Article 4 (Transitional provision) A review carried out before this scheme takes effect that meets the requirements of Article 7 is regarded as a review under this scheme.

Article 5 (Revision of other guidelines) With the commencement of this scheme, the relevant parts of related guidelines are revised.

Commentary on the Addenda

The transitional provisions mean that contracts already concluded need not all be changed at once. They can be brought into line at renewal.

A business that has been reviewing on its own before commencement can use those records as they are. The four things Article 7 requires must, however, be shown in the record.

[Annex Table 1] Counting permanent employees

The number of permanent employees is the sum of the headcount on the last day of each month of the previous business year, divided by the number of months.

Dispatched workers are not counted. Part-time workers are counted in proportion to their working hours.

[Annex Table 2] Range that a certification audit may substitute

An item confirmed in an information security management system certification audit may substitute the review of the corresponding item among the Article 7 review items.

Even where substituted, the audit result on which the substitution rests must be kept with the review record.

[Annex Table 3] Handling status review record form

Date of review / Reviewer / Scope of review / Excluded scope and reason

Result by item (confirmed · could not confirm · not applicable)

Matters found / Action taken / Planned date of action

Responsible person's confirmation

— End —