ARTICLE 29 DATA PROTECTION WORKING PARTY

第29條個資保護工作小組

17/EN

WP 253

Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679

關於第2016/679號規則(GDPR)中的行政罰鍰適用和制定之指引

Adopted on 3 October 2017

2017年10月3日通過

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

本工作小組係依據95/46/EC指令第29條設立。為歐洲資料保護與隱私之獨立諮詢機構。其任務規範於95/46/EC指令第30條及2002/58/EC指令第15條。

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 03/075.

由歐盟執委會司法總署C署（基本權利與歐盟公民）擔任秘書處，其地址為比利時，布魯塞爾B-1049，第MO-59 03/075號辦公室。

Website: http://ec.europa.eu/justice/data-protection/index_en.htm

網址：http://ec.europa.eu/justice/data-protection/index_en.htm

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

關於個人資料運用*之個資保護工作小組

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, having regard to Articles 29 and 30 thereof,

having regard to its Rules of Procedure,

依歐洲議會與歐盟理事會1995年10月24日之第95/46/EC號指令而設立，

基於該指令第29條及第30條，

基於其程序規則，

HAS ADOPTED THE PRESENT GUIDELINES:

通過此份指引：

＊譯註：我國個資法將個資之使用分為蒐集(collection)、處理(processing)、利用(use)等不同行為態樣，且有相應之適用要件，而GDPR對個資之蒐集、處理、利用任一行為，皆統稱為 processing。為與我國個資法中之「處理」有所區隔，本文因此將GDPR中的processing 譯為「運用」，processor 譯為「受託運用者」。

Table of contents 目錄

I. Introduction
導言

The EU has completed a comprehensive reform of data protection regulation in Europe. The reform rests on several pillars (key components): coherent rules, simplified procedures, coordinated actions, user involvement, more effective information and stronger enforcement powers.

歐盟已完成歐洲資料保護規則的全面性改革。此改革係基於幾項支柱（關鍵構成要素）：一致性之規則、簡化之程序、協調之行動、使用者之參與、更有效之資訊及更強大之執法權力。

Data controllers and data processors have increased responsibilities to ensure that personal data of the individuals is protected effectively. Supervisory authorities have powers to ensure that the principles of the General Data Protection Regulation (hereafter 'the Regulation') as well as the rights of the individuals concerned are upheld according to the wording and the spirit of the Regulation.

資料控管者和資料受託運用者被附加了更多的責任，以確保有效保護當事人之個人資料。監管機關有權確保一般資料保護規則（以下簡稱「本規則」）之原則及相關之個人權利，已依據本規則之文義和精神予以維護。

Consistent enforcement of the data protection rules is central to a harmonized data protection regime. Administrative fines are a central element in the new enforcement regime introduced by the Regulation, being a powerful part of the enforcement toolbox of the supervisory authorities together with the other measures provided by article 58.

資料保護規則的一致性執法是調和資料保護制度之核心。行政罰鍰係本規則所引進新執法制度之核心要素，另加上第58條規定之其他措施，構成監管機關有力之執法工具。

This document is intended for use by the supervisory authorities to ensure better application and enforcement of the Regulation and expresses their common understanding of the provisions of article 83 of the Regulation as well as its interplay with articles 58 and 70 and their corresponding recitals.

本文件旨在提供監管機關使用，以確保更好地適用和執行本規則，並表達監管機關對本規則第83條規定之共識，以及與第58條、第70條和相對應前言間之適用關係。

In particular, according to article 70, (1) (e), the European Data Protection Board (hereafter 'EDPB') is empowered to issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation and article 70, (1), (k) specifies the provision for guidelines concerning the setting of administrative fines.

尤其是，依據第70條第1項第e款，歐洲個人資料保護委員會（以下簡稱「EDPB」）有權

發布指引、建議和優良實務做法，以促進本規則適用之一致性，且第70條第1項第k款明定關於設定行政罰鍰之指引的規定。

These guidelines are not exhaustive, neither will they provide explanations about the differences between administrative, civil or criminal law systems when imposing administrative sanctions in general.

本指引並非詳盡無遺，且亦不會對行政、民事或刑事法律制度在一般課以行政處罰時之差異作出解釋。

In order to achieve a consistent approach to the imposition of the administrative fines, which adequately reflects all of the principles in these guidelines, the EDPB has agreed on a common understanding of the assessment criteria in article 83 (2) of the Regulation and therefore the EDPB and individual supervisory authorities agree on using this Guideline as a common approach.

為充分反映這些指引中之所有原則，以一致性之方式裁處行政罰鍰，EDPB已對本規則第83條第2項中之評估標準達成共識，因此EDPB和個別監管機關均同意以本指引作為共同的方法。

II. Principles
原則

Once an infringement of the Regulation has been established based on the assessment of the facts of the case, the competent supervisory authority must identify the most appropriate corrective measure(s) in order to address the infringement. The provisions of article 58 (2) b-j[1] indicate which tools the supervisory authorities may employ in order to address non-compliance from a controller or a processor. When using these powers, the supervisory authorities must observe the following principles:

一旦依據案件事實之評估而確認違反本規則，權責監管機關必須識別最合適之矯正措施以因應違反之情況。第58條第2項第b-j款[1]之規定表明監管機關可採用何種工具以因應控管者或受託運用者不合規之情形。當行使這些權力時，監管機關必須遵守以下原則：

1. Infringement of the Regulation should lead to the imposition of "equivalent sanctions".
違反本規則應處以「同等之制裁」。

The concept of "equivalence" is central in determining the extent of the obligations of the supervisory authorities to ensure consistency in their use of corrective powers according to article 58 (2) in general, and the application of administrative fines in particular[2].

「同等」之概念於決定監管機關之責任範圍時為主要核心，以確保監管機關依據第58條第2項行使矯正權之一致性，尤其是行政罰鍰之適用範圍，[2]。

In *order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union**, the level of protection should be equivalent** in all Member States* (recital 10). Recital 11 elaborates the fact that an equivalent level of protection of personal data throughout the Union requires, amongst others, "*equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States.*". Further more,

[1] Article 58 (2) a provides that warnings may be issued when "processing operations are likely to infringe provisions of the Regulation". In other words, in the case covered by the provision the infringement of the Regulation has not occurred yet.
第58條第2項第a款規定，當「運用作業可能違反本規則之條款」時，可發出警告。易言之，在該條款所涵蓋之範圍內，尚未發生違反本規則之情況。

[2] Even where the legal systems in some EU countries do not allow for the imposition of administrative fines as set out in the Regulation, such an application of the rules in those Member States needs to have an equivalent effect to administrative fines imposed by supervisory authorities (recital 151). The Courts are bound by the Regulation but they are not bound by these guidelines of the EDPB.
即使某些歐盟國家的法律制度不允許處以本規則所規定之行政罰鍰，惟當這些成員國適用該國法規時，仍需與監管機關得處以之行政罰鍰效果相當（前言第151點）。法院受本規則之約束，但不受這些EDPB指引之約束。

equivalent sanctions in all Member States as well as effective cooperation between supervisory authorities of different Member States is seen as a way "*to prevent divergences hampering the free movement of personal data within the internal market*", in line with recital 13 of the Regulation.

*為了確保對自然人一致性和高標準之保護，並移除歐盟境內個人資料流通之阻礙，所有成員國應提供**同等程度之保護**（前言第10點）*。前言第11點中亦詳述，對歐盟境內個人資料提供同等程度之保護須有「*同等程度之權力以監控和確保個人資料保護規則之遵守，以及成員國對違反行為有同等程度之制裁*」。此外，所有成員國之同等制裁以及不同成員國監管機關間之有效合作被視為係「*防止分歧阻礙個人資料在內部市場自由流通*」之方式，此與本規則前言第13點一致。

The Regulation sets a stronger basis than Directive 95/46/EC for a greater level of consistency as the Regulation is directly applicable in the Member States. While supervisory authorities operate with "complete independence" (article 52) with respect to national governments, controllers or processors, they are required to cooperate "*with a view to ensuring the consistency of application and enforcement of this Regulation*" (article 57, (1),(g)).

由於本規則可直接適用於成員國，因此本規則制定了比第95/46/EC號指令更強力之基礎，以實現更大程度之一致性。雖然監管機關作業「完全獨立」（第52條）於國家政府、控管者或受託運用者，然其被要求必須相互合作「*以確保本規則適用和執法之一致性*」（第57條第1項第g款）。

The Regulation calls for a greater consistency than the Directive 95/46 when imposing sanctions. In cross border cases, consistency shall be achieved primarily through the cooperation (one–stop-shop) mechanism and to some extent through the consistency mechanism set forth by the new Regulation.

在施以制裁時，本規則要求比第95/46號指令更大程度之一致性。就跨境案件而言，一致性應主要係透過合作（一站式）機制，並在一定程度上透過新規則所規定之一致性機制始得以實現。

In national cases covered by the Regulation, the supervisory authorities will apply these guidelines in the spirit of cooperation according to article 57, 1 (g) and article 63, with a view to ensuring the consistency of application and enforcement of the Regulation. Although supervisory authorities remain independent in their choice of the corrective measures presented in Article 58 (2), it should be avoided that different corrective measures are chosen by the supervisory authorities in similar cases.

就本規則所涵蓋之成員國案件而言，監管機關將依據第57條第1項第g款和第63條之合作精神適用這些指引，以確保本規則適用和執法之一致性。雖然監管機關在選擇第58條第2項

規定之矯正措施時仍保持獨立，但應避免監管機關在類似案件中，選擇不同之矯正措施。

The same principle applies when such corrective measures are imposed in the form of fines.
當以罰鍰形式執行此類矯正措施時，適用相同之原則。

---

2. *Like all corrective measures chosen by the supervisory authorities, administrative fines should be "effective, proportionate and dissuasive".*
行政罰款與監管機關所選擇之所有矯正措施相同，必須「有效性、合比例性與具勸阻性」。

Like all corrective measures in general, administrative fines should adequately respond to the nature, gravity and consequences of the breach, and supervisory authorities must assess all the facts of the case in a manner that is consistent and objectively justified. The assessment of what is effective, proportional and dissuasive in each case will have to also reflect the objective pursued by the corrective measure chosen, that is either to reestablish compliance with the rules, or to punish unlawful behavior (or both).
與一般所有矯正措施相同，行政罰鍰應足以反應侵害之性質、嚴重程度和後果，監管機關必須以一致且客觀合理之方式評估案件所有事實。在每個案件中，評估何者為有效性、合比例性與具勸阻性時，亦須反映所選擇之矯正措施追求的目標，即欲重新建立對規則之遵守，或欲處罰違法之行為（或兩者）。

Supervisory authorities should identify a corrective measure that is "*effective, proportionate and* dissuasive" (art. 83 (1)), both in national cases (article 55) and in cases involving cross- border processing of personal data (as defined in article 4 (23)).
監管機關應在成員國之案件（第55條）和涉及跨境運用個人資料之案件中（如第4條第23款之定義）識別出「*有效性、合比例性與具勸阻性*」之矯正措施（第83條第1項）。

These guidelines recognize that national legislation may set additional requirements on the enforcement procedure to be followed by the supervisory authorities. This may for example include address notifications, form, deadlines for making representations, appeal, enforcement, payment[3].
這些指引認識到國家立法可能對監管機關應遵循之執法程序設置額外要求。可能包括如：發出通知、格式、指定代理人期限、上訴、執行、支付[3]。

[3] As an example, the constitutional framework and draft data protection legislation of Ireland, provides that a formal decision is reached on the fact of the infringement itself, which is communicated to the relevant parties, before an assessment of the scale of the sanction(s). The decision on the fact of the infringement itself cannot be revisited during the assessment of the scale of the sanction(s).
例如，愛爾蘭的憲法框架和資料保護立法草案規定，在對制裁範圍進行評估前，須就違反事實本身作出正式決定，並將其傳達予相關各方。在評估制裁範圍時，不得重新審查違反事實本身之決定。

Such requirements should however not hinder in practice the achievement of effectiveness, proportionality or dissuasiveness.

然而，這些要求在實務上不應妨礙有效性、合比例性或具勸阻性之實現。

A more precise determination of effectiveness, proportionality or dissuasiveness will be generated by emerging practice within supervisory authorities (on data protection, as well as lessons learned from other regulatory sectors) as well as case-law when interpreting these principles.

監管機關之實務做法（關於資料保護和從其他監管部門汲取之經驗）以及解釋這些原則之判例法，將對有效性、合比例性或具勸阻性產生更精準之判斷。

In order to impose fines that are effective, proportionate and dissuasive, the supervisory authority shall use for the definition of the notion of an undertaking as provided for by the CJEU for the purposes of the application of Article 101 and 102 TFEU, namely that the concept of an undertaking **is understood to mean** an economic unit, which may be formed by the parent company and all involved subsidiaries. In accordance with EU law and case-law[4], an undertaking must be understood to be the economic unit, which engages in commercial/economic activities, regardless of the legal person involved (Recital 150).

為使裁處之罰鍰具有效性、合比例性與勸阻性，監管機關應使用歐盟法院為適用歐盟基本條約第101條和第102條之目的而對企業之概念所為之定義，即該企業之概念**應理解為**一個可由母公司和所有相關子公司組成之經濟單位。依據歐盟法律和判例法[4]，企業必須被理解為從事商業/經濟活動之經濟單位，無論是否涉及法人（前言第150點）。

---

3. The competent supervisory authority will make an assessment "in each individual case".
權責監管機關將「於每一個案件中」進行評估。

Administrative fines may be imposed in response to a wide range of infringements. Article 83 of the Regulation provides a harmonized approach to breaches of obligations expressly listed in paras (4)-(6). Member State law may extend the application of article 83 to public authorities

[4] The ECJ case law definition is: «the concept of an undertaking encompasses every entity engaged in an economic activity regardless of the legal status of the entity and the way in which it is financed" (Case Höfner and Elsner, para 21, ECLI:EU:C:1991:161). An undertaking «must be understood as designating an economic unit even if in law that economic unit consists of several persons, natural or legal» (Case Confederación Española de Empresarios de Estaciones de Servicio [para 40, ECLI:EU:C:2006:784).
歐洲法院判例法之定義為：「企業之概念包括從事經濟活動的每個實體，無論該實體之法律地位及其融資方式為何」（CaseHöfner和Elsner，第21段，ECLI：EU：C：1991：161）。企業「必須被理解為一個指定的經濟單位，即使在法律定義下該經濟單位係由多人組成，無論是自然人或法人」（西班牙服務據點營運商聯合會案例，第40段，ECLI:EU:C:2006:784）。

and bodies established in that Member State. Additionally, Member State law may allow for or even mandate the imposition of a fine for infringement of other provisions than those mentioned in article 83 (4)-(6).

針對各種違反行為皆有處以行政罰鍰之可能。本規則第83條對違反第4－6項明確列舉之義務提供了一種一致性之處理方式。成員國法律可擴大第83條的適用範圍至設立於該成員國境內之公務機關和機構。此外，成員國法律可允許或甚至授權對於違反第83條第4－6項以外之其他規定處以罰鍰。

The Regulation requires assessment of each case individually[5]. Article 83 (2) is the starting point for such an individual assessment. The paragraph states "*when deciding whether to impose an administrative fine, and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following…*"Accordingly, and also in the light of Recital 148[6] the supervisory authority has the responsibility of choosing the most appropriate measure(s). In the cases mentioned in Article 83 (4) – (6), this choice **must** include consideration of all of the corrective measures, which would include consideration of the imposition of the appropriate administrative fine, either accompanying a corrective measure under Article 58(2) or on its own.

本規則要求個別評估每一案件[5]。第83條第2項係此類個案評估之起始點。該項規定「*在決定是否處以行政罰鍰，且於個案中對行政罰鍰之金額作出決定時，應就以下要件給予適當之考量.....*」。因此，且依據前言第148點[6]，監管機關有責任選擇最合適之措施。在第83

[5] Further to the application of article 83 criteria there are other provisions to bolster the foundation of this approach such as:

除第83條標準之適用外，尚有其他條款支持此種方式之基礎，例如

- recital 141 "*the investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case*."
  前言第141點「*申訴後之調查應在符合司法審查之具體個案的適當範圍中進行。*」
- recital 129 "*The powers of supervisory authorities should be exercised in accordance with appropriate procedural safeguards set out in Union and Member State law, impartially, fairly and within a reasonable time. In particular each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case…*".
  前言第129點「*監管機關權力之行使應依據歐盟和成員國法律所規定之適當程序性安全維護措施，在合理時間內以公平且公正之方式為之。尤其是，考量到每個案件的具體情況，為確保對本規則之遵守，每項措施皆應為適當的、必要的及合比例性…。*」
- article 57(1) (f) "*handle complaints lodged by a data subject, or by a body, organisation or association in accordance with article 8(應為第Article 80), and investigate to the extent appropriate, the subject matter of the complaint*."
  第57條第1項第f款「處理當事人或機構、組織或協會依據第80條提出之申訴，並在適當的範圍內調查該申訴事項。」

[6] "*In order to strengthen the enforcement of the rules of this Regulation, penalties including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation. In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine. Due regard should however be given to the nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory*

條第4－6項所提及之情況下，此種選擇**必須**包括考量所有矯正措施，其中包括考量單獨處以適當之行政罰鍰，或併行採取第58條第2項規定之矯正措施。

Fines are an important tool that supervisory authorities should use in appropriate circumstances. The supervisory authorities are encouraged to use a considered and balanced approach in their use of corrective measures, in order to achieve both an effective and dissuasive as well as a proportionate reaction to the breach. The point is to not qualify the fines as last resort, nor to shy away from issuing fines, but on the other hand not to use them in such a way which would devalue their effectiveness as a tool.

罰鍰係監管機關在適當情況下應使用之重要工具。鼓勵監管機關在實施矯正措施時採用經過深思熟慮且平衡之方式，以便達到對侵害行為施以有效性、具勸阻性以及合比例性之回應。關鍵為不將罰鍰視為最後手段，亦非避免罰鍰，但另一方面，罰鍰之使用不應減低其作為重要工具之有效性。

The EDPB, when competent according to article 65 of the Regulation, will issue a binding decision on disputes between authorities relating in particular to the determination of the existence of an infringement. When the relevant and reasoned objection raises the issue of the compliance of the corrective measure with the GDPR, the decision of EDPB will also discuss how the principles of effectiveness, proportionality and deterrence are observed in the administrative fine proposed in the draft decision of the competent supervisory authority. EDPB guidance on the application of article 65 of the Regulation will follow separately for further detail on the type of decision to be taken by the EDPB.

當符合本規則第65條之規定時，EDPB將就機關間，尤其是關於是否存在違反行為之爭議，做出具有約束力之決定。當對矯正措施是否符合GDPR提出相關及合理之異議時，EDPB亦將討論權責監管機關初步決定建議之行政罰鍰如何遵守有效性、合比例性與具勸阻性原則並做決定。EDPB關於適用本規則第65條之指導將另外進一步詳細說明EDPB可採取決定之類型。

---

authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor. The imposition of penalties including administrative fines should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including effective judicial protection and due process".

「*為加強本規則法規之執行，除了或代替監管機關依據本規則所採取之適當措施外，應對違反本規則之行為處以包括行政罰鍰等之處罰。若僅是輕微之違反或可能被處以之罰鍰對自然人構成不成比例之負擔時，得採用告誡之方式取代罰鍰。但應適當考量違反之性質、嚴重程度和持續期間、違反之故意性、為減輕所受損害而採取之行動、責任程度或先前任何相關之違反、監管機關獲知該違反行為之方式、遵守針對控管者或受託運用者之命令措施、遵守行為守則以及其他任何加重或減輕之要素。裁處包括行政罰鍰之處罰應遵守符合歐盟法及(歐洲聯盟基本權利憲章)憲章中一般原則之適當程序性安全維護措施，包括有效之司法保護及正當程序*」。

4. *A harmonized approach to administrative fines in the field of data protection requires active participation and information exchange among Supervisory Authorities*
為就資料保護領域之行政罰鍰採取協調一致之方法，需監管機關相互間之積極參與和資訊交流

These guidelines acknowledge that fining powers represent for some national supervisory authorities a novelty in the field of data protection, raising numerous issues in terms of resources, organization and procedure. Notably, the decisions in which the supervisory authorities exercise the fining powers conferred to them will be subject to appeal before national courts.

本指引承認，對某些國家監管機關而言，罰鍰權是資料保護領域的新穎經驗，且在資源、組織和程序方面引起了許多問題。值得注意的是，監管機關行使被賦予之罰鍰權而為之決定可上訴於國家法院。

Supervisory authorities shall cooperate with each other and where relevant, with the European Commission through the cooperation mechanisms as set out in the Regulation in order to support formal and informal information exchanges, such as through regular workshops. This cooperation would focus on their experience and practice in the application of the fining powers to ultimately achieve greater consistency.

監管機關應透過本規則規定之合作機制相互合作，且在需要時與歐盟執委會合作，並透過定期研討會等方式，以維持正式和非正式之資訊交流。此種合作將側重於監管機關在應用罰鍰權方面之經驗和實務做法，以最終實現更大程度之一致性。

This proactive information sharing, in addition to emerging case law on the use of these powers, may lead to the principles or the particular details of these guidelines being revisited.

此種主動的資訊共享，以及行使這些權力之新判例法，可能導致本指引之原則或具體細節被重新審視。

III. Assessment criteria in article 83 (2)
第83條第2項中之評估標準

Article 83 (2) provides a list of criteria the supervisory authorities are expected to use in the assessment both of whether a fine should be imposed and of the amount of the fine. This does not recommend a repeated assessment of the same criteria, but an assessment that takes into account all the circumstances of each individual case, as provided by article 83[7].

第83條第2項提供了監管機關在評估是否應處以罰鍰和罰鍰金額時應使用之標準清單。在此不建議相同標準之重複評估，而是建議依據第83條之規定，考量每一個案之所有情況[7]後之一次性評估。

The conclusions reached in the first stage of the assessment may be used in the second part concerning the amount of the fine, thereby avoiding the need to assess using the same criteria twice.

在第一階段評估中得出之結論可在關於罰鍰金額的第二階段中援用，從而避免使用相同之標準評估二次。

This section provides guidance for the supervisory authorities of how to interpret the individual facts of the case in the light of the criteria in article 83 (2).

本章節為監管機關提供指導，以瞭解如何依據第83條第2項之標準解釋案件之個別事實。

(a) the nature, gravity and duration of the infringement
違反之性質、嚴重程度和持續期間

Almost all of the obligations of the controllers and processors according to the Regulation are categorised according to their **nature** in the provisions of article 83(4) – (6). The Regulation, in setting up two different maximum amounts of administrative fine (10/20 million Euros), already indicates that a breach of some provisions of the Regulation may be more serious than for other provisions. However the competent supervisory authority, by assessing the facts of the case in light of the general criteria provided in article 83 (2), may decide that in the particular case there is a higher or a more reduced need to react with a corrective measure in

[7] The assessment of the sanction to be applied may come separately after the assessment of whether there has been an infringement due to national procedural rules arising from constitutional requirements in some countries. Therefore, this may limit the content and the amount of detail in a draft decision issued by lead supervisory authority in such countries.

因某些國家憲法要求之國家程序法，對所適用制裁方法之評估，可能係於評估是否有違反行為之後，單獨進行。因此，可能會限制這些國家的主責監管機關發布草擬決定之內容和細節數量。

the form of a fine. Where a fine has been chosen as the one or one of several appropriate corrective measure(s), the tiering system of the Regulation (article 83 (4)- 83 (6)) will be applied in order to identify the maximum fine that can be imposed according to the nature of the infringement in question.

依據本規則，幾乎所有控管者和受託運用者之義務皆依據其**性質**，於第83條第4－6項中加以分類。本規則制定兩種不同之行政罰鍰金額上限（1/2千萬歐元），以指出違反本規則某些條款可能比違反其他條款更加嚴重。然而，權責監管機關在依據第83條第2項規定之一般標準評估案件事實時，可決定在特定個案中是否需要以裁處罰鍰形式作為矯正措施。當罰鍰被選擇為一種或其中一種適當的矯正措施時，將適用本規則之層級化體系（第83條第4項－83條第6項），以確認依據系爭違反性質可裁處之最高罰鍰金額。

Recital 148 introduces the notion of "minor infringements". Such infringements may constitute breaches of one or several of the Regulation's provisions listed in article 83 (4) or (5). The assessment of the criteria in article 83 (2) may however lead the supervisory authority to believe that in the concrete circumstances of the case, the breach for example, does not pose a significant risk to the rights of the data subjects concerned and does not affect the essence of the obligation in question. In such cases, the fine may (but not always) be replaced by a reprimand.

前言第148點引進了「輕微違反」之概念。此類違反行為可能構成違反第83條第4項或第5項中所列一項或多項之規定。然而，第83條第2項之評估標準可能使監管機關認為，在案件的具體情狀下，例如，侵害行為未對相關當事人之權利造成重大風險，亦未影響系爭義務之實質面。在此類案件中，罰鍰或許（但非總是）可被告誡取代。

Recital 148 does not contain an obligation for the supervisory authority to always replace a fine by a reprimand in the case of a minor infringement ("*a reprimand may be issued instead of a fine*"), but rather a possibility that is at hand, following a concrete assessment of all the circumstances of the case.

前言第148點並無規定監管機關有義務在輕微違反之情況下必須以告誡取代罰鍰（「*可能予以告誡而非裁處罰鍰*」），而是對案件所有情狀具體評估後，一種可能之選擇。

Recital 148 opens up the same possibility to replace a fine by a reprimand, where the data controller is a natural person and the fine likely to be imposed would constitute a disproportionate burden. The starting point is that the supervisory authority has to assess whether, considering the circumstances of the case at hand, the imposition of a fine is required. If it finds in favour of imposing a fine, then the supervisory authority must also assess whether the fine to be imposed would constitute a disproportionate burden to a natural

person.

當資料控管者為自然人且可能被處以之罰鍰將造成不成比例之負擔時，前言第148點開啟了以告誡取代罰鍰之相同可能性。起始點仍為監管機關必須依據當前案件之情況，評估是否需處以罰鍰。若監管機關認為需處以罰鍰，則其亦必須評估所處以之罰鍰是否會對自然人構成不成比例之負擔。

Specific infringements are not given a specific price tag in the Regulation, only a cap (maximum amount). This can be indicative of a relative lower degree of gravity for a breach of obligations listed in article 83(4), compared with those set out in article 83(5). The effective, proportionate and dissuasive reaction to a breach of article 83(5) will however depend on the circumstances of the case.

本規則並未對特定違反行為給予具體之價格標籤，而只定有上限（最高金額）。相較於第83條第5項，對第83條第4項所列義務之違反，嚴重程度相對較低。然而，就違反第83條第5項所為之有效性、符合比例性與具勸阻性之回應方式，仍將取決於案件之具體情況。

It should be noticed that breaches of the Regulation, which by their nature might fall into the category of "up to 10 million Euros or up to 2% of total annual worldwide turnover" as set out in article 83 (4), might end up qualifying for a higher tier (Euro 20 million) category in certain circumstances. This would be likely to be the case where such breaches have previously been addressed in an order from the supervisory authority, an order[8] which the controller or processor failed to comply with[9] (article 83 (6)). The provisions of the national law may in practice have an impact on this assessment[10]. The nature of the infringement, but also "*the scope, purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them*", will be indicative of the **gravity** of the infringement. The occurrence of several different infringements committed together in any particular single case means that the supervisory authority is able to apply the administrative fines at a level which is effective, proportionate and dissuasive within the limit of the gravest infringement. Therefore, if an infringement of article 8 and article 12 has been discovered, then the supervisory authority may be able to apply the corrective measures as set out in article 83(5) which correspond to the category of the gravest infringement, namely article 12. More detail at this stage is beyond the scope of this particular guideline (as detailed calculation work would be the focus of a potential subsequent stage of this guideline).

應注意的是，違反本規則之行為，依其性質，可能落入第83條第4項規定「最高1000萬歐元或全球年度總營業額2%」之類別，在某些情況下，亦可能被歸類於更高金額（2000

萬歐元）之類別。此種情況很可能是監管機關已於先前之命令[8]中指出了此種違反行為，而控管者或受託運用者未能遵守其命令[9]（第83條第6項）。國家法律規定實際上可能會對此一評估產生影響[10]。違反之性質，以及「*相關運用之範圍和目的、受影響當事人之人數以及當事人受損害之程度*」，皆能指出違反之**嚴重程度**。在任何特定案件中同時發生若干不同違反行為時，監管機關得在最嚴重之違反行為的限制範圍內裁處有效性、合比例性與具勸阻性之行政罰鍰。因此，若發現違反第8條和第12條之行為，則監管機關可採取第83條第5項規定之矯正措施，以因應第12條所列之最嚴重違反行為種類。本階段之進一步細節已超出本指引之範圍（詳盡之計算工作將係本指引可能之後續階段重點）。

The factors below should be assessed in combination eg. the number of data subjects together

---

[8] The orders, provided in article 58 (2) are:
第58條第2項規定之命令為：

- to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;
  命令控管者或受託運用者遵守當事人依據本規則行使其權利之要求；
- to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;
  命令控管者或受託運用者，如適當，以特定方式並在規定期限內使運用作業符合本規則之規定；
- to order the controller to communicate a personal data breach to the data subject;
  命令控管者將個人資料侵害資訊傳達予當事人；
- to impose a temporary or definitive limitation including a ban on processing
  施以臨時或最終之限制，包括禁止運用
- to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;
  依據第16、17和18條命令更正或刪除個人資料或限制運用，並依據第17條第2項和第19條向被揭露個人資料之接收者發出此類行動之通知；
- to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;
  命令認證機構撤銷依據第42條和第43條核發之認證，或命令認證機構不得核發認證，若未能滿足或不再符合認證要求。
- to order the suspension of data flows to a recipient in a third country or to an international organisation.
  命令暫停資料傳輸至第三國之接收者或國際組織。

[9] Application of article 83(6) necessarily must take into account national law on procedure. National law determines how an order is issued, how it is notified, from which point it takes effect, whether there is a grace period to work on compliance. Notably, the effect of an appeal on the enforceability of an order should be taken into account.
第83條第6項之適用於程序上必須考量到國家法律。國家法律決定命令如何發布、如何通知、從何時起生效、是否存在合規性之寬限期。值得注意者為，應考量上訴對命令可執行性之影響。

[10] Statutory provisions of limitation may have the effect that a previous order of the supervisory authority may no longer be taken in to consideration due to the amount of time that has lapsed since that previous order was issued. In some jurisdictions, rules require that after the prescription period has passed with respect to an order, no fine may be imposed for non-compliance with that order under article 83(6). It will be up to each supervisory authority in each jurisdiction to determine how such impacts will affect them.
法定限制條款可能會導致不須考量監管機關先前之命令，因該命令自發布以來已經過一定之時間。在某些管轄權內，法規要求當命令之時效經過後，對於不遵守第83條第6項下之命令不得處以罰鍰。此將由每一管轄權內之每個監管機關來認定這些衝突對其自身之影響。

with the possible impact on them.
以下因素應結合評估，例如，當事人之人數以及可能對其產生之影響。

The number of data subjects involved should be assessed, in order to identify whether this is an isolated event or symptomatic of a more systemic breach or lack of adequate routines in place. This is not to say that isolated events should not be enforceable, as an isolated event could still affect a lot of data subjects. This will, depending on the circumstances of the case, be relative to, for example, the total number of registrants in the database in question, the number of users of a service, the number of customers, or in relation to the population of the country, as appropriate.
應評估所涉及當事人之人**數**，以辨別此為獨立事件，或是系統性侵害的徵兆，或缺乏適當常規程序。此非謂不可對獨立事件執法，因單一事件仍可影響許多當事人。依據案件具體情況，此將與，例如，系爭資料庫註冊者總數、一項服務的用戶數量、消費者數量相關，或於適當情況下，與國家人口數相關。

The purpose of the processing must also be assessed. The WP 29 opinion on "purpose limitation"[11] previously analysed the two main building blocks of this principle in data protection law: purpose specification and compatible use. When assessing the purpose of the processing in the context of article 83 (2), the supervisory authorities should look into the extent to which the processing upholds the two key components of this principle[12]. In certain situations, the supervisory authority might find it necessary to factor in a deeper analysis of the purpose of the processing in itself in the analysis of article 83 (2).
運用之**目的**亦須被納入評估。29條工作小組先前關於「目的限制」[11]之意見分析了資料保護法中此一原則的兩個主要組成部分：目的明確性和用途相容性。在第83條第2項範圍內評估運用目的時，監管機關應考量該運用在多大程度上可維護本原則的兩個關鍵組成部分[12]。在特定情況下，監管機關可能發現有必要在分析第83條第2項時更深入地解析運用本身之目的。

If the data subjects have suffered **damage**, the level of the damage has to be taken into consideration. Processing of personal data may generate risks for the rights and freedoms of

[11] WP 203 , Opinion 03/2013 on purpose limitation, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf
第03/2013號意見，關於目的限制，WP 203，請查詢 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf。
[12] See also WP 217, opinion 6/2014 on the notion of legitimate interest of the data controller under article 7, page 24, on the question: "What makes an interest "legitimate" or "illegitimate"?"
另請參閱，第6/2014號意見，關於第7條資料控管者正當利益之概念，WP 217，第24頁，關於：「什麼使利益『正當』或『不正當』?」之問題。

the individual, as illustrated by recital 75:

若當事人遭受**損害**，則必須考量其損害程度。運用個人資料可能會對當事人之權利和自由產生風險，如前言第75點所述：

> *"The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non- material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects."*
>
> *「個人資料運用可能導致自然人的權利及自由產生不同可能性與嚴重性的風險，恐造成人身、財物或非財物的損害，尤其是：在運用可能導致歧視、身分冒用或詐欺、財務損失、聲譽受損、受職業秘密保護的個人資料之秘密性喪失、未經授權的假名化回溯、或任何其他重大經濟性或社會性之不利益時；在當事人可能被剝奪其權利和自由或被禁止對其個人資料行使控制權時；在運用個人資料將揭露種族或民族、政治觀點、宗教或哲學信仰、工會會員資格、基因資料運用、健康資料或有關性生活或刑事前科和犯罪或相關安全措施之資料時；在涉及評估個人面向，尤其是分析或預測有關工作表現、經濟情況、健康、個人偏好或興趣、可靠性或行為、所在位置或移動，以建立或使用個人資料檔案時；在運用弱勢自然人，尤其是兒童之個人資料時；或在運用涉及大量個人資料並影響大量當事人時。」*

If damages have been or are likely to be suffered due to the infringement of the Regulation

then the supervisory authority should take this into account in its choice of corrective measure, although the supervisory authority itself is not competent to award the specific compensation for the damage suffered.
若因違反本規則而已經或可能受到損害，則監管機關在選擇矯正措施時應就此情形加以考量，儘管監管機關本身並無權就所遭受之損害給予具體賠償。

The imposition of a fine is not dependent on the ability of the supervisory authority to establish a causal link between the breach and the material loss (see for example article 83 (6)).
罰鍰之課處並不取決於監管機關在侵害和實質損害間建立因果關係之能力（請參閱例如第83條第6項）。

Duration of the infringement may be illustrative of, for example:
違反之**持續期間**可說明，例如：

a) wilful conduct on the data controller's part, or
資料控管者之故意行為，或

b) failure to take appropriate preventive measures, or
未採取適當之預防措施，或

c) inability to put in place the required technical and organisational measures.
無能力實施所需之技術性和組織性措施。

(b) the intentional or negligent character of the infringement
違反行為之故意或過失

In general, "intent" includes both knowledge and wilfulness in relation to the characteristics of an offence, whereas "unintentional" means that there was no intention to cause the infringement although the controller/processor breached the duty of care which is required in the law.
一般說來，「故意」包含對違法行為相關要素之知悉和意欲，而「非故意」意味著雖然控管者/受託運用者違反了法律規定之注意義務，然卻無意造成該違反行為。

It is generally admitted that intentional breaches, demonstrating contempt for the provisions of the law, are more severe than unintentional ones and therefore may be more likely to warrant the application of an administrative fine. The relevant conclusions about wilfulness or negligence will be drawn on the basis of identifying objective elements of conduct gathered

from the facts of the case. In addition, emergent case law and practice in the field of data protection under the application of the Regulation will be illustrative of circumstances indicating clearer thresholds for assessing whether a breach was intentional.
一般普遍承認，故意違法，表示對法律規定之蔑視，比非故意違法更為嚴重，因此更有可能被處以行政罰鍰。其結果為故意或過失，將以該案件事實之行為客觀要素判斷。此外，就本規則之適用，資料保護領域下之新判例法和實務作法將在評估是否為故意違法時，提供更明確之門檻。

Circumstances indicative of intentional breaches might be unlawful processing authorised explicitly by the top management hierarchy of the controller, or in spite of advice from the data protection officer or in disregard for existing policies, for example obtaining and processing data about employees at a competitor with an intention to discredit that competitor in the market.
認定為故意違反之情狀可能包含來自於控管者最高管理層級明確授權之非法運用，或儘管個資保護長已提出建議或根本無視現有政策，例如意圖使市場上的競爭對手失去信譽而取得及運用競爭對手之員工資料。

Other examples here might be:
其他之示例可能為：

- amending personal data to give a misleading (positive) impression about whether targets have been met – we have seen this in the context of targets for hospital waiting times
  修改個人資料，以對是否達成目標做出誤導性（積極）之印象–我們曾在關於「醫院候診時間之目標」見到此種情況。

- the trade of personal data for marketing purpose ie selling data as 'opted in' without checking/disregarding data subjects' views about how their data should be used
  基於行銷目的交易個人資料，即未檢視/漠視當事人關於如何使用其資料之觀點，預設當事人選擇同意出售資料。

Other circumstances, such as failure to read and abide by existing policies, human error, failure to check for personal data in information published, failure to apply technical updates in a timely manner, failure to adopt policies (rather than simply failure to apply them)may be indicative of negligence.
其他情狀，例如未能閱讀和遵守現有政策、人為錯誤、未能檢查公布資訊中之個人資料、

未能及時實施技術性更新、未能採行政策（而非單純的不加以應用），可能認定為過失。

Enterprises should be responsible for adopting structures and resources adequate to the nature and complexity of their business. As such, controllers and processors cannot legitimise breaches of data protection law by claiming a shortage of resources. Routines and documentation of processing activities follow a risk-based approach according to the Regulation.

企業應有責任採行適合其業務性質和複雜性之結構及資源。因此，控管者和受託運用者不得藉由聲稱資源短缺以正當化其違反資料保護法之行為。運用活動之例行程序和文件記錄須依據本規則以風險為基礎之方式為之。

There are grey areas which will affect decision-making in relation to whether or not to impose a corrective measure and the authority may need to do more extensive investigation to ascertain the facts of the case and to ensure that all specific circumstances of each individual case were sufficiently taken into account.

某些灰色地帶會影響是否採取矯正措施之決定，而機關可能需要進行更廣泛之調查，以確認案件事實，並確保充分考量到每個案件的所有具體情況。

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

控管者或受託運用者為減輕當事人所遭受之損害而採取的任何行動；

The data controllers and processors have an obligation to implement technical and organisational measures to ensure a level of security appropriate to the risk, to carry out data protection impact assessments and mitigate risks arising form the processing of personal data to the rights and freedoms of the individuals. However, when a breach occurs and the data subject has suffered damage, the responsible party should do whatever they can do in order to reduce the consequences of the breach for the individual(s) concerned. Such responsible behaviour (or the lack of it) would be taken into account by the supervisory authority in their choice of corrective measure(s) as well as in the calculation of the sanction to be imposed in the specific case.

資料控管者和受託運用者有義務實施技術性和組織性措施，以確保適合風險之安全層級、辦理個資保護影響評估、並減輕運用個人資料對當事人權利和自由所造成之風險。然而，若發生侵害且當事人受到損害時，責任方應該盡其所能，以減輕該侵害行為對相關當事人之後果。監管機關在選擇矯正措施以及計算特定案件中之懲罰金額時，將考量此種負責任（或不負責任）之行為。

Although aggravating and mitigating factors are particularly suited to fine-tune the amount of a fine to the particular circumstances of the case, their role in the choice of appropriate corrective measure should not be underestimated. In cases where the assessment based on other criteria leaves the supervisory authority in doubt about the appropriateness of an administrative fine, as a standalone corrective measure, or in combination with other measures in article 58, such aggravating or attenuating circumstances may help to choose the appropriate measures by tipping the balance in favour of what proves more effective, proportionate and dissuasive in the given case.

雖然加重和減輕因素特別適合於依據案件之特定情況微調罰鍰金額，但不應低估其在選擇適當矯正措施中之作用。若基於其他標準的評估使監管機關對行政罰鍰之適當性有疑義時，例如應採一項單獨之矯正措施或併同第58條中其他措施，在特定案件中，此種加重或減輕情形藉由衡量哪種措施較有效性、合比例性與具勸阻性，可能有助於適當措施之選擇。

This provision acts as an assessment of the degree of responsibility of the controller after the infringement has occurred. It may cover cases where the controller/processor has clearly not taken a reckless/ negligent approach but where they have done all they can to correct their actions when they became aware of the infringement.

本條款作用在違反行為發生後，對控管者責任程度之評估。該條款可能涵蓋當控管者/受託運用者顯然沒有重大過失/過失之作為，且在意識到侵害發生時，已盡其所能改正其行為之情況。

Regulatory experience from SAs under the 95/46/EC Directive has previously shown that it can be appropriate to show some degree of flexibility to those data controllers/processors who have admitted to their infringement and taken responsibility to correct or limit the impact of their actions. This might include examples such as (although this would not lead to a more flexible approach in every case):

監管機關先前在第95/46/EC號指令下之SA監管經驗已顯示出，對於已承認違反行為，並負責改正或限縮其行為所造成之影響的資料控管者/受託運用者，表現出某種程度之彈性是適當的。此可能包括之示例如（雖然這不會導致每個案件都適用更彈性方式）：

- contacting other controllers/processors who may have been involved in an extension of the processing e.g. if there has been a piece of data mistakenly shared with third parties.

  聯繫可能涉及延伸運用之其他控管者/受託運用者，例如曾誤與第三方分享一些資料。

- timely action taken by the data controller/processor to stop the infringement from continuing or expanding to a level or phase which would have had a far more serious impact than it did.
  資料控管者/受託運用者即時採取行動，以阻止侵害繼續或擴大至產生更嚴重影響之程度。

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;
控管者或受託運用者之責任程度，需考量到其依據第25條和第32條所執行之技術性和組織性措施；

The Regulation has introduced a far greater level of accountability of the data controller in comparison with the EC Data Protection Directive 95/46/EC.
與第95/46/EC號資料保護指令相較，本規則就資料控管者之課責性採用更高層級之規定。

The degree of responsibility of the controller or processor assessed against the backdrop of applying an appropriate corrective measure may include:
以採行適當矯正措施為背景評估控管者或受託運用者之責任程度，可能包括：

- Has the controller implemented technical measures that follow the principles of data protection by design or by default (article 25)?
  控管者是否已執行符合資料保護設計或預設原則之技術性措施（第25條）？
- Has the controller implemented organisational measures that give effect to the principles of data protection by design and by default (article 25) at all levels of the organisation?
  控管者是否已在組織內各個層級皆已執行資料保護設計或預設原則之組織性措施（第25條）？
- Has the controller/processor implemented an appropriate level of security (article 32)?
  控管者/受託運用者是否已落實適當之安全程度（第32條）？
- Are the relevant data protection routines/policies known and applied at the appropriate level of management in the organisation? (Article 24).
  組織之適當管理層級是否已知曉並適用相關資料保護例行程序/政策？（第24條）。

Article 25 and article 32 of the Regulation require that the controllers "*take into account the state of the art, the cost of implementation and the nature, scope, context, and purposes of the processing, as well as the risks of varying likelihood and severity for rights and freedoms for the natural persons posed by the processing*". Rather than being an obligation of goal, these provisions introduce obligations of means, that is, the controller must make the necessary assessments and reach the appropriate conclusions. The question that the supervisory authority must then answer is to what extent the controller "did what it could be expected to do" given the nature, the purposes or the size of the processing, seen in light of the obligations imposed on them by the Regulation.

本規則第25條和第32條要求控管者「*考量現有技術、執行成本和運用之性質、範圍、背景與目的，以及運用對自然人權利和自由所造成風險之各種不同可能性和嚴重性*」。這些規定並非目標式之義務，而係引進方法式之義務，即控管者必須進行必要之評估並得出適當之結論。因此，監管機關必須回答的問題為，依本規則賦予之義務，於何種程度可認控管者依運用之性質、目的或規模「已做到其所被期待做到的事情」。

In this assessment, due account should be taken of any "best practice" procedures or methods where these exist and apply. Industry standards, as well as codes of conduct in the respective field or profession are important to take into account. Codes of practice might give an indication as to what is common practice in the field and an indication of the level of knowledge about different means to address typical security issues associated with the processing.

在本評估中，應適當考量現有和適用之任何「最佳實務」程序或方法。產業標準以及各別領域或專業中之行為守則係重要之考量因素。實務守則可提供某個領域中通用做法指標，及以不同方法解決與運用相關之典型安全議題之認知程度指標。

While best practice should be the ideal to pursue in general, the special circumstances of each individual case must be taken into account when making the assessment of the degree of responsibility.

一般來說，雖然最佳實務做法應是追求之理想，但在評估責任程度時，必須考量每個案件之特殊情況。

(e) any relevant previous infringements by the controller or processor;

控管者或受託運用者先前任何相關之違反行為；

This criterion is meant to assess the track record of the entity committing the infringement. Supervisory authorities should consider that the scope of the assessment here can be quite

wide because any type of breach of the Regulation, though different in nature to the one being investigated now by the supervisory authority might be "relevant" for the assessment, as it could be indicative of a general level of insufficient knowledge or disregard for the data protection rules.

本標準旨在評估實體違反行為之追蹤記錄。監管機關應考量到此處之評估範圍可能是非常廣泛的，因任何違反本規則之行為，即便性質可能與監管機關正在調查者不同，惟因其可顯示未充分知悉或未注意資料保護規則之總體情況，因此，仍可能與該評估「相關」。

The supervisory authority should assess:

監管機關應評估：

- Has the controller/processor committed the same infringement earlier?
  控管者/受託運用者過去是否曾犯過相同之違反行為？
- Has the controller/processor committed an infringement of the Regulation in the same manner? (for example as a consequence of insufficient knowledge of existing routines in the organisation, or as a consequence of inappropriate risk assessment, not being responsive to requests from the data subject in a timely manner, unjustified delay in responding to requests and so on).
  控管者/受託運用者是否以同樣之方式違反了本規則？（例如，由於對組織中現有慣例之認知不足，或由於不適當之風險評估、未能即時回應當事人之要求、對要求不合理的延遲回應等）。

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
與監管機關之配合程度，以補救違反行為並減輕其可能產生之不利影響；

Article 83 (2) provides that the degree of cooperation may be given "due regard" when deciding whether to impose an administrative fine and in deciding on the amount of the fine. The Regulation does not give a precise answer to the question how to take into account the efforts of the controllers or the processors to remedy an infringement already established by the supervisory authority. Moreover, it is clear that the criteria would usually be applied when calculating the amount of the fine to be imposed.

第83條第2項規定，在決定是否處以行政罰鍰和決定罰鍰金額時，可「適當考量」配合程度。就如何考量控管者或受託運用者為補救經監管機關確認之違反行為所做的努力之問題，本規則並未提供明確答案。此外，很明顯的，在計算課處之罰鍰金額時通常會適

用此標準。

However, where intervention of the controller has had the effect that negative consequences on the rights of the individuals did not produce or had a more limited impact than they could have otherwise done, this could also be taken into account in the choice of corrective measure that is proportionate in the individual case.
然而，若控管者之干預所造成之影響並未對當事人權利產生負面後果或產生比預期更有限之影響，在個案中選擇合比例性之矯正措施時，亦可納入考量。

One example of a case where cooperation with the supervisory authority might be relevant to consider might be:
考慮與監管機關配合之可能相關示例為：

- Has the entity responded in a particular manner to the supervisory authority's requests during the investigation phase in that specific case which has significantly limited the impact on individuals' rights as a result?
  在特定案件的調查階段，該實體是否以特別之方式回應監管機關之要求，從而大幅度限縮了對個人權利之影響？

This said, it would not be appropriate to give additional regard to cooperation that is already required by law for example, the entity is in any case required to allow the supervisory authority access to premises for audits/inspections.
意即，對於法律已要求之配合並不適宜給予額外之關注，例如，在任何情況下，實體本需允許監管機關進入其營業處所進行稽核/檢查。

(g) the categories of the personal data affected by the infringement;
受違反行為影響之個人資料類型；

Some examples of key questions that the supervisory authority may find it necessary to answer here, if appropriate to the case, are:
若於該案件適合之情形，監管機關可能認為有必要回答之關鍵問題示例為：

- Does the infringement concern processing of special categories of data set out in articles 9 or 10 of the Regulation?
  違反行為是否涉及運用本規則第9條或第10條規定之特種資料？
- Is the data directly identifiable/ indirectly identifiable?
  資料是否可直接/間接識別？

- Does the processing involve data whose dissemination would cause immediate damage/distress to the individual (which falls outside the category of article 9 or 10)?
  運用是否涉及散播會對個人造成直接損害/痛苦之資料（並非屬第9條或第10條之類型）？

- Is the data directly available without technical protections, or is it encrypted[13]?
  資料是否無技術性保護而可直接使用，或者已加密[13]？

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;
監管機關得知違反行為之方式，尤其係控管者或受託運用者是否就該違反行為進行通知以及通知之程度為何；

A supervisory authority might become aware about the infringement as a result of investigation, complaints, articles in the press, anonymous tips or notification by the data controller. The controller has an obligation according to the Regulation to notify the supervisory authority about personal data breaches. Where the controller merely fulfils this obligation, compliance with the obligation cannot be interpreted as an attenuating/ mitigating factor. Similarly, a data controller/processor who acted carelessly without notifying, or at least not notifying all of the details of the infringement due to a failure to adequately assess the extent of the infringement may also be considered by the supervisory authority to merit a more serious penalty i.e. it is unlikely to be classified as a minor infringement.
監管機關可能透過調查、申訴、新聞文章、匿名舉報或資料控管者之通知得知違反行為。依據本規則，控管者有義務向監管機關通知個人資料侵害事件。若控管者僅履行此義務，尚不得將遵守該義務解釋為減弱/減輕因素。同樣的，若資料控管者/受託運用者由於不注意而未能通知，或由於沒有充分評估違反行為之程度而未能通知違反行為之所有細節時，監管機關可考量較嚴厲之懲罰，即不太可能被歸類為輕微之違反行為。

(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;
若先前已基於相同爭議，向該控管者或受託運用者就第58條第2項所述措施發布命

[13] It shouldn't always be considered 'a bonus' mitigating factor that the breach only concerns indirectly identifiable or even pseudonymous/encrypted data. For those breaches, an overall assessment of the other criteria might give a moderate or strong indication that a fine should be imposed.
即使侵害僅涉及可間接識別之資料或甚至為假名化/加密資料，此情形不應被視為一種「紅利」減輕要素。對於這些侵害行為，其他標準之總體評估可能會得出適度或強烈之指標，顯示應處以罰鍰。

令，其遵循該措施之情形如何；

A controller or processor may already be on the supervisory authority's radar for monitoring their compliance after a previous infringement and contacts with the DPO where they exist are likely to have been extensive. Therefore, the supervisory authority will take into account the previous contacts.

在先前之違反行為後，監管機關可能已在雷達上監控控管者或受託運用者的法遵情形，並與個資保護長（如有）密切聯繫。因此，監管機關將考量先前之聯繫狀況。

As opposed to the criteria in (e), this assessment criteria only seeks to remind supervisory authorities to refer to measures that they themselves have previously issued to the same controller or processors "*with regard to the same subject matter*".

與第（e）項中之標準相反，此評估標準之目的僅為提醒監管機關考量其先前已向同一控管者或受託運用者「*基於相同爭議*」所實施之措施。

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42;

遵守依據第40條認可之行為守則或依據第42條認可之認證機制；

Supervisory authorities have a duty to "*monitor and enforce the application of this* Regulation, (article 57 1 (a))". Adherence to approved codes of conduct may be used by the controller or processor as an way to demonstrate compliance, according to articles 24 (3), 28 (5) or 32 (3).

監管機關有責任「*監督和執行本規則之適用*（第57條第1項第a款）」。依據第24條第3項、第28條第5項或第32條第3項，控管者或受託運用者可使用經認可之行為守則作為證明其合規性之方式。

In case of a breach of one of the provisions of the Regulation, adherence to an approved code of conduct might be indicative of how comprehensive the need is to intervene with an effective, proportionate, dissuasive administrative fine or other corrective measure from the supervisory authority. Approved codes of conduct will, according to article 40 (4) contain "*mechanisms which enable the (monitoring) body to carry out mandatory monitoring of compliance with its provisions*".

當違反本規則之其中一項規定時，依據已認可的行為守則，可能會使監管機關需要全面的採取有效性、合比例性與具勸阻性的行政罰款或其他糾正措施介入干預。依據第40條第4項，經認可之行為守則將包含「*相關機制使（監督）機構得對遵守其規定進行強制性之監督*」。

Where the controller or processor has adhered to an approved code of conduct, the supervisory authority may be satisfied that the code community in charge of administering the code takes the appropriate action themselves against their member, for example through the monitoring and enforcement schemes of the code of conduct itself. Therefore, the supervisory authority might consider that such measures are effective, proportionate or dissuasive enough in that particular case without the need for imposing additional measures from the supervisory authority itself. Certain forms of sanctioning non-compliant behaviour may be made through the monitoring scheme, according to article 41 (2) c and 42 (4), including suspension or exclusion of the controller or processor concerned from the code community. Nevertheless, the powers of the monitoring body are "*without prejudice to the tasks and powers of the competent supervisory authority*", which means that the supervisory authority is not under an obligation to take into account previously imposed sanctions pertaining to the self-regulatory scheme.

當控管者或受託運用者遵守經認可之行為守則時，監管機關或許可信賴負責管理守則之守則社群對其成員採取適當之行動，例如透過對行為守則本身之監督和執行計畫。因此，監管機關可能會認為這些措施於該特定情況下是屬有效性、合比例性或具勸阻性，而無需由監管機關本身施以額外之措施。依據第41條第2項第c款及42條第4項，可透過監督計畫對違規行為處以某些形式之懲罰，包括暫停或取消相關控管者或受託運用者於守則社群之資格。然而，監督機構之權力「*不得損害權責監管機關之任務和權力*」，此意味著監管機關並無義務考量自我監督計畫先前所實施之懲罰。

Non-compliance with self-regulatory measures could also reveal the controller's/processor's negligence or intentional behaviour of non-compliance.

不遵守自我監督措施亦可顯示控管者/受託運用者之過失或故意不遵守之行為。

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

適用於案件情狀之任何其他加重或減輕因素，例如直接或間接從違反行為中獲得經濟利益或避免損失。

The provision itself gives examples of which other elements might be taken into account when deciding the appropriateness of an administrative fine for an infringement of the provisions mentioned in Article 83(4-6).

該條款本身舉例說明了在決定因違反第83條第4-6項所述條款，而處以行政罰鍰之適當性時，可將其他因素納入考量。

Information about profit obtained as a result of a breach may be particularly important for the supervisory authorities as economic gain from the infringement cannot be compensated through measures that do not have a pecuniary component. As such, the fact that the controller had profited from the infringement of the Regulation may constitute a strong indication that a fine should be imposed.

因侵害而獲利之資訊對於監管機關而言可能尤其重要，因違反行為帶來的經濟利益無法透過非金錢之措施得到補償。因此，控管者從違反本規則中獲利之事實可能成為應處以罰鍰之強大指標。

IV. Conclusion
結論

Reflections on the questions such as those provided in the previous section will help supervisory authorities identify, from the relevant facts of the case, those criteria which are most useful in reaching a decision on whether to impose an appropriate administrative fine in addition to or instead of other measures under Article 58. Taking into account the context provided by such assessment, the supervisory authority will identify the most effective, proportionate and dissuasive corrective measure to respond to the breach.
對上述章節所提供問題之反思將有助於監管機關從案件的相關事實中識別出最有效用之標準，以決定在除了或替代第58條所規定其他措施之情況下，是否處以適當之行政罰鍰。考量此類評估所提供之脈絡，監管機關將識別出最有效性、合比例性與具勸誡性之矯正措施，以回應違反行為。

Article 58 provides some guidance as to which measures a supervisory authority might choose, as the corrective measures in themselves are different in nature and suited primarily for achieving different purposes. Some of the measures in article 58 may even be possible to cumulate, therefore achieving a regulatory action comprising more than one corrective measure.
第58條就監管機關可選擇之措施提供了一些指導，因矯正措施本身性質之不相同，且根本上適合不同目的之達成。第58條中所列舉之某些措施甚至可疊加適用，因此實現了包含一種以上矯正措施之監管行動。

It is not always necessary to supplement the measure through the use of another corrective measure. For example: The effectiveness and dissuasiveness of the intervention by the supervisory authority with its due consideration of what is proportionate to that specific case may be achieved through the fine alone.
並非總是需要使用另一措施來補充矯正措施。例如：監管機關以比例性適當考量特定案件情況，可能僅須透過罰鍰即可使干預行為具有效性及勸阻性。

In essence, authorities need to restore compliance through all of the corrective measures available to them. Supervisory authorities will also be required to choose the most appropriate channel for pursuing regulatory action. For example, this could include penal sanctions (where these are available at national level).
原則上，機關需透過所有可使用之矯正措施以恢復合規性。監管機關亦將被要求選擇最適合採取之監管行動管道。例如，此可能包括刑事處分（當此規範於成員國國內法時）。

The practice of applying administrative fines consistently across the European Union is an evolving art. Actions should be taken by supervisory authorities working together to improve consistency on an ongoing basis. This can be achieved through regular exchanges through case-handling workshops or other events which allow the comparison of cases from the sub-national, national and cross-border levels. The creation of a permanent sub-group attached to a relevant part of the EDPB is recommended to support this ongoing activity.

於歐盟內實施一致性行政罰鍰之做法仍是一門持續發展的藝術。監管機關應採取行動，共同努力，在現有基礎上不斷提升一致性。此可透過案件處理研討會或其他活動進行定期交流得以實現，這些活動可對來自地方、國家和跨境層級之案例進行比較。建議成立一個隸屬於EDPB相關部門之永久性小組以支援此項持續進行之活動。