**Procedure No: E/07781/2020**
IMI Reference: Case Register **177442**

FINAL DECISION TO DISCONTINUE PROCEEDINGS

From the actions carried out by the Spanish Data Protection Agency and based on the following

FACTS

FIRST: On 28 September 2020, the investigation was initiated as a result of an analysis of a letter notifying a personal data breach, sent by TEKA INDUSTRIAL, S.A with VAT A39004932 (hereinafter TEKA), informing the Spanish Data Protection Agency, on 24 August 2020, of the following: TEKA belongs to the HERITAGE-B group and has suffered a security breach resulting from a ***ransomware attack*** affecting various entities of the Group located in different countries, including TEKA. It also states that there are group companies in Germany, France, the United Kingdom, Switzerland and Mexico. The HERITAGE-B Group has notified the AEPD and the German Authority as it considers that they are the countries where the main establishments of the group are located.

SECOND: The 'Internal Market Information System' (hereinafter 'the IMI system'), governed by Regulation (EU) No 1024/2012 of the European Parliament and of the Council of 25 October 2012 (the IMI Regulation), aims to promote cross-border administrative cooperation, mutual assistance between Member States and the exchange of information. Via the IMI system (A56ID 175553), on 20 January 2021 the Spanish Agency declared itself the lead authority in this case, pursuant to Article 4 (23) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27/04/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR), since TEKA has one of its main establishments in Spain.

According to the information entered into the IMI system, in accordance with Article 60 of the GDPR, act as concerned supervisory authorities in this case the supervisory authorities of: Berlin (Germany), Baden-Württemberg (Germany), Bavaria — Private sector (Germany), France and Mecklenburg-Western Pomerania (Germany). All of them under Article 4 (22) GDPR, given that data subjects residing in these Member States are substantially affected or are likely to be substantially affected by the processing at issue in these proceedings.

THIRD: The General Subdirectorate of Data Inspection carried out preliminary investigations in order to establish a possible infringement of data protection legislation, becoming aware of the following:

On 27 October 2020, information was requested from TEKA and the reply received shows the following:

With regard to the company

— TEKA is a company belonging to the HERITAGE-B corporate group which manufactures, sales and distributes products made from special steels. TEKA is the lead company in three distinct business lines: kitchens, baths and containers.

TEKA is considered to be the lead entity of the HERITAGE-B Group in so far as certain relevant decisions relating to information systems are taken by the HERITAGE-B Group.

***— The Group's main provider is Microsoft Ireland Operations Limited, with whom TEKA has a framework service contract in the European region.***

***TEKA stated that the systems where the breach had occurred were maintained internally by the Group's IT teams.***

With regard to the chronology of the events

***— On 3 August 2020, a suspicious activity began with the creation of an administrator account in the group's corporate systems.***

***— On 5 August the first suspicious behaviour appeared with several attempts to connect on the corporate network and the execution of the first malicious file.***

***— Tools and services are installed between 5 and 21 August 2020 using an interface and preparing the environment for further exploitation.***

***— On 21 August 2020 ransomware was implemented throughout the corporate network.***

***TEKA states that the detection took place on 21 August and immediately activated a monitoring system (expert cybersecurity teams of Telefónica) to monitor the activity of the systems and detect, where appropriate, any other suspicious activity.***

On the causes that made the security breach possible

— The ***entrance of the attackers to TEKA's systems took place through the theft of user accounts by phishing and the discovery of passwords by gross force (testing and error of millions of combinations to gain access).***

***Once within the corporate network, movements were detected using legitimate credentials of remote desktop applications.***

Measures to minimise the impact of the security breach and actions taken for final resolution

***— On 21 August, TEKA closed the servers and isolated the systems to contain the cyber-attack and contracted Telefónica to carry out a forensic analysis of the incident.***

***— Immediately, technical measures were taken at network level and other measures such as the retrieval and security of the servers concerned or the activation of existing backups.***

***— At the same time, Telefónica carried out constant real-time monitoring, carrying out, inter alia, the analysis of access records (log), system analysis and network traffic analysis.***

***Senior management, legal and IT teams were also involved in the incident analysis to create contingency plans and take appropriate measures in each business unit.***

With regard to the data concerned

***— The number of people affected is around 2.000, of which 569 are Spanish and the other countries of the European Union and third countries.***

***— The data affected by the Incident were mostly corporate data (TEKA's business is aimed at the sale of business-to-business products and services — business to business B2B — and therefore customers and suppliers are generally legal persons).***

***TEKA considers that the attack was not aimed at obtaining personal data but at business information.***

***The categories of data concerned are: basic identification data, ID card/NIE/passport, access or identification credentials, economic or financial data, contact details and business and company information.***

***— TEKA states that they have monitored the activity after the security breach and is not aware of any malicious use by the attackers.***

***However, the publication on the darkweb — on 16 September — of certain information affected by the incident was immediately identified and all links to the incident were quickly disabled, so it is estimated that the information was only accessible for the minimum time needed to disable those links (approximately 1 hour).***

***On 23 August, TEKA carried out a risk analysis in accordance with the model included in the Guide on the Management and notification of security breachs published by the AEPD, which concluded, on the basis of the technical and forensic information available on that date, that the incident did not pose a high risk to the rights of those affected, whereas the incident consisted mainly of encryption of data — mainly corporate — and the use of data by third parties had not been identified. TEKA therefore decided, on the basis of the available information, that there was no need to notify the data subjects about the incident.***

***— On 17 September, TEKA carried out a second risk analysis with more information and after it had been identified that certain data had been provided as a result of the incident and had been published on the darkweb in order to verify what action should be taken as a result of these findings.***

***On the basis of the information available on 17 September, TEKA determined that such exfiltration did not pose a high risk to the rights of those affected by Teka's business and activity in so far as the information published was mostly corporate and access to it had been prevented within 1 hour of its publication.***

***Notwithstanding the above, the analysis was made not only for TEKA but also for the other entities in the group. As a result of that analysis, certain German group entities affected by the incident (namely KEK GmbH, THIELMANN UCON GmbH and THIELMANN WEW GmbH) did determine, by the nature of the potentially compromised information concerning their organisations, that it was appropriate to notify those employees whose bank details had been compromised as a result of the incident in order to recommend them to take appropriate measures and avoid being subject to fraud or other similar criminal activity.***

***— TEKA states that it aims to maintain a dynamic and continuous risk assessment (which takes into account the updated information at every stage of the process and is revised in the event of new findings), granular and detailed, which involves maintaining open lines of communication with the authorities, and a detailed analysis of whether or not it is necessary to communicate the security breach to data subjects in accordance with the AEPD and other authorities methodology, so that communication has been made in the relevant cases.***

With regard to security measures implemented prior to the security breach

***— TEKA has a strict policy against phishing and carries out frequent awareness-raising campaigns for its employees through informative emails, both preventive and warning against specific phishing attempts against the organisation on aspects of the company's technological use policy.***

***The procedures provided to address such threats define the protocol to be followed for the notification and handling of such security incidents.***

***In that regard, TEKA has provided a copy of the explanatory emails on phishing and the protocol to be followed 'Protection against cyber-attacks'.***

***TEKA has also provided the document 'HERITAGE Group's Information Technology Use Policy'. This document contains the Annexes: 'IT Acceptance and Authorisation for Personal Devices Form'.***

***It includes, inter alia,the policy for passwords, internet usage and personal devices.***

***— TEKA has provided the following documents:***

> ***— Copy of the Register of Processing Activities where the reported security breach has occurred.***
>
> ***— Security policy (HERITAGE Group's Information Technology Use Policy).***

***— Back-up manual.***

***— Procedure for the registration, removal and modification of user permits.***

***— Emails classification policy according to their level of protection***

***— Phishing protection policy.***

***— Register of access to the anonymised Data Processing Centre.***

***— Security breach management procedure***

With regard to measures implemented after the security breach

***— As a result of the incident, in order to strengthen its security measures and to be able to monitor its efficiency, TEKA has hired the company SECURE & IT to carry out a specific audit of the security elements of the Group. This company will also provide maintenance services to deal with incidents.***

***— Procurement of tools with Microsoft and the management and monitoring of these tools with certified partners similar to Telefónica.***

***— TEKA is currently reviewing and updating all its security measures, including its policies. The following measures have been taken after the Incident:***

***— Strengthening access control***

***— Complexity of passwords and shortening of the renewal period;***

***—Sessions analysis on a more regular basis;***

***— General prohibition of the use of personal devices (only allowed in exceptional cases);***

***— Monitoring the use of unauthorised applications;***

***— Use of authorised file sharing tools only***

***— Reinforcement of recommendations on sending sensitive information (personal data, confidential data, etc.) in encrypted attachments and, in general, security awareness campaigns among employees.***

Information on the recurrence of these events and the number of similar events occurring over time

***— TEKA has no evidence of a recurrence of facts relating to the incident.***

FOURTH: On 02 September 2021, the Director of the AEPD adopted a draft decision to discontinue the proceedings. On the same day, following the process set out in Article 60 of the GDPR, the draft decision to discontinue the proceedings was shared in IMI and

the concerned supervisory authorities were informed that they had four weeks from that time to raise relevant and reasoned objections. During the expiry of the period for that purpose, the concerned supervisory authorities did not raise relevant and reasoned objections in that regard, and therefore all the supervisory authorities were deemed to agree with and were bound by that draft decision, in accordance with Article 60(6) GDPR.

## LEGAL GROUNDS

### I
### Competence

In accordance with the powers of investigation and corrective powers conferred on each supervisory authority by Article 58 of Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter GDPR), and in accordance with Article 47 of the Spanish Organic Law 3/2018 of 5 December 1995 on the protection of personal data and the guarantee of digital rights (hereinafter LOPDGDD), the Director of the Spanish Data Protection Agency is competent for deciding on these procedure.

### II
### Preliminary remarks

Article 4.12 GDPR defines 'personal data breaches' (hereinafter "security breach") as *'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.*

In the present case, it is common ground that there was a personal data security breach in the circumstances set out above, categorised as a confidentiality breach, as a result of a ***ransomware attack affecting TEKA***.

It should be noted that reporting a personal data security breach does not entail the imposition of a penalty directly, as it is necessary to analyse the diligence of controllers and processors and the security measures applied.

The security of personal data is regulated by Articles 32, 33 and 34 GDPR, which regulate the security of the processing, the notification of a personal data security breach to the supervisory authority, as well as the communication to the data subject.

### III
### Article 32 GDPR

Recital (39) of the GDPR states that:

*'(…) Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing'.*

In this regard, Article 32 *'Security of* processing' of the GDPR provides:

*"1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*
*(a) pseudonymisation and encryption of personal data;*
*(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*
*(c) the ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident;*
*(D) a process of regular verification, assessment and assessment of the effectiveness of technical and organisational measures to ensure the security of the processing.*

*2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.*

*3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.*

*4. The controller and the processor shall take measures to ensure that any person acting under the authority of the controller or of the processor who has access to personal data may process such data only on instructions from the controller, unless required to do so by Union or Member State law."*

*'1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*

*(a) the pseudonymisation and encryption of personal data;*
*(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*
*(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;*
*(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.*

*2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.*

*3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.*

*4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law'.*

***In the present case, prior to the security breach under consideration, TEKA already had a strict policy against phishing and carried out frequent awareness-raising campaigns for its employees by means of information emails, both preventive and warning of specific phishing attempts detected against the organisation on aspects of the company's technological use policy. Despite this, attackers were able to enter TEKA's systems through the theft of user accounts by phishing and the discovery of passwords by raw force (testing and mistake of millions of combinations to gain access).***

***While on 3 August 2020 started a suspicious activity with the creation of an administrator account in the Group's corporate systems, it is not until 21 August 2020 that ransomware is executed across the corporate network, which is when TEKA became aware that the security incident had occurred. On the same day, TEKA closed the servers and isolates the systems to contain the cyber-attack and contracted Telefónica to perform a forensic analysis of the incident. Technical measures were immediately taken at network level and other measures such as retrieval and securitisation of affected servers or activation of existing backups. At the same time, Telefónica carried out constant and real-time monitoring, carrying out, inter alia, the analysis of access records (log), system analysis and network traffic analysis. Senior management, legal and IT teams were also involved in the incident analysis to create contingency plans and take appropriate measures in each business unit.***

***As a result of the incident, TEKA has contracted SECURE & IT to carry out a specific audit of the Group's security features. This company will also provide maintenance services to deal with incidents.***

***Tools have also been contracted with Microsoft and commissioned the management and monitoring of these tools to certified partners similar to Telefónica.***

***In addition, TEKA is currently reviewing and updating all its security measures, including its policies, and the following measures have been taken:***

- ***— Strengthening access control***
- ***— Complexity of passwords and shortening of the renewal period;***
- ***— Sessions analysis on a more regular basis;***
- ***— General prohibition of the use of personal devices (only allowed in exceptional cases);***
- ***— Monitoring the use of unauthorised applications;***
- ***— Use of authorised file sharing tools only***
- ***— Reinforcement of recommendations on sending sensitive information (personal data, confidential data, etc.) in encrypted attachments and, in general, security awareness campaigns among employees.***

In the present case, it is not apparent from the documents provided by TEKA in the course of these investigations that, prior to the security breach, TEKA did not have reasonable security measures on the basis of the estimated potential risks.

Furthermore, there is no evidence that it did not act diligently once the security breach had been known, nor that the measures taken after the incident in question were inadequate.

There are also no complaints to this Agency from data subjects relating to the present security breach.

IV
Article 33 GDPR

Recital (85) of the GDPR states that:

*'A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay'.*

In that regard, Article 33 *'Notification of a personal data breach to the supervisory authority'* of the GDPR provides:

*'1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.*

*2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.*

*3. The notification referred to in paragraph 1 shall at least:*

*(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;*

*(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;*

*(c) describe the likely consequences of the personal data breach;*
*(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.*

*4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.*

*5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.'*

In the present case, TEKA notified the security breach within the period laid down in the GDPR for that purpose, with the information set out in Article 33 of the GDPR.

V
Article 34 GDPR

Recital (86) of the GDPR states that:

*"The controller should communicate the personal data breach to the data subject without undue delay if it may result in a high risk to his or her rights and freedoms and allow him or her to take the necessary precautions. The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate a risk of immediate damage would justify swift communication with data subjects, while it can be justified that communication takes longer because of the need to implement appropriate measures to prevent continuous or similar personal data breaches."*

*'The controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions. The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data* breaches may justify more time for communication'

In this regard, Article *34 'Communication of a personal data breach to the data subject'* of the GDPR *provides:*

*"1. Where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay. L 119/52 ES Official Journal of the European Union 4.5.2016*

*2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).*

*3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met: (a) the controller has put in place appropriate technical and organisational protection measures and these measures have been applied to the personal data concerned by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; (b) the controller has taken further steps to ensure that the high risk to the rights and freedoms of the data subject referred to in paragraph 1 is no longer likely to materialise; (c) involves a disproportionate effort. In such a case, there shall instead be a public communication or a similar measure whereby the data subjects are informed in an equally effective manner.*

*4. Where the controller has not yet communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach leading to a high risk, may require the data subject to do so or may decide that one of the conditions referred to in paragraph 3 is fulfilled."*

*'1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.*

*2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).*

*3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:*

> *(a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;*
> *(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;*
> *(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.*

*4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data*

*breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met'.*

***In the present case, the number of people affected is around 2.000, of which 569 are Spanish and the rest of the other countries of the European Union and third countries.***

***However, the data affected by the incident were mostly corporate data, as TEKA's business is aimed at the sale of business-to-business products and services — business to business B2B — and therefore customers and suppliers are generally legal persons. In addition, TEKA considers that the attack was not aimed at obtaining personal data but at business information. On 23 August 2020, TEKA carried out a risk analysis in accordance with the model included in the Guide on the management and reporting of security breaches published by the AEPD, which concluded, on the basis of the technical and forensic information available on that date, that the incident did not pose a high risk to the rights of data subjects, whereas the incident mainly consisted of encryption of data — predominantly corporate — and the use of data by third parties had not been identified. TEKA therefore decided, on the basis of the available information, that there was no need to notify the data subjects about the incident.***

***Subsequently, TEKA identified on 16 September 2020 the publication on the darkweb of certain information affected by the incident and all links to the incident were quickly disabled, so it is estimated that the information was only accessible for the minimum time needed to disable those links (approximately 1 hour).***

***On 17 September 2020, TEKA carried out a second risk analysis with more information and found that such exfiltration did not pose a high risk to the rights of those affected by TEKA's business and activity in so far as the information published was mostly corporate and access to it had been prevented within 1 hour of its publication.***

***However, the analysis was made not only for TEKA but also for the other entities in the group. As a result of that analysis, certain German group entities affected by the incident (namely KEK GmbH, THIELMANN UCON GmbH and THIELMANN WEW GmbH) did determine, by the nature of the potentially compromised information concerning their organisations, that it was appropriate to notify those employees whose bank details had been compromised as a result of the incident in order to recommend them to take appropriate measures and avoid being subject to fraud or other similar criminal activity.***

In the present case, the security breach was not likely to result in a high risk to the rights and freedoms of natural persons, with the result that TEKA was not required to communicate to the data subjects that a security breach had occurred, within the meaning of Article 34 of the GDPR.

It should be noted that this AEPD has no complaints from potential victims.

VI
No infringement

Therefore, on the basis of the above paragraphs, no evidence has been found to prove the existence of an infringement within the remit of the Spanish Data Protection Agency.

In accordance with the above, the Director of the Spanish Data Protection Agency therefore:
AGREED TO:

FIRST: DISCONTINUE the present actions.

SECOND: Notify this decision to TEKA INDUSTRIAL, S.A.

In accordance with Article 50 of the Spanish LOPDGDD, this Resolution will be made public once it has been notified to the interested parties.

In accordance with Article 114.1 (c) and with Articles 112 and 123 of Spanish Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations, the parties concerned may lodge an appeal with the Director of the Spanish Data Protection Agency within one month of the day following notification of this decision or a direct administrative appeal to the Administrative Appeals Chamber of the National High Court, in accordance with Article 25 and paragraph 5 of the Fourth Additional Provision of Spanish Law 29/1998 of 13 July governing the Administrative Jurisdiction, within two months of the day following notification of this act, as provided for in Article 46 (1) of that Law.

940-010921

Mar España Martí
Director of the AEPD, P.O., General Subdirectorate of Data Inspection, [redacted] Resolution 4 October 2021