In the matter of the General Data Protection Regulation

DPC Case Reference: IN-21-6-2

In the matter of A&G Couriers Limited T/A Fastway Couriers (Ireland)

Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act 2018

Further to an own-volition inquiry commenced pursuant to Section 110 of the Data Protection Act 2018

DECISION

Decision-Maker for the Data Protection Commission:

Helen Dixon
Commissioner for Data Protection

30 December 2022

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Contents

1. Introduction

1.1 This document (**'the Decision'**) is a decision made by the Data Protection Commission (**'the DPC'**) in accordance with section 111 of the Data Protection Act 2018 (**'the 2018 Act'**). I make this Decision having considered the information obtained in the own volition inquiry (**'the Inquiry'**) pursuant to section 110 of the 2018 Act.

1.2 A&G Couriers Limited T/A Fastway Couriers (Ireland) ('**Fastway'**) was provided with a Draft Decision (**'the Draft Decision'**) on this Inquiry on 11 April 2022 to give it final opportunity to make submissions. This Decision is being provided to Fastway pursuant to section 116(1)(a) of the 2018 Act in order to give Fastway notice of the Decision, the reasons for it, and the corrective powers that I have decided to exercise.

1.3 This Decision contains corrective powers under section 115 of the 2018 Act and Article 58(2) of the General Data Protection Regulation (**'the GDPR'**) arising from the infringements which have been identified herein. In this regard, Fastway is required to comply with these corrective powers.

2. Legal Framework for the Inquiry and the Decision

i. Legal Basis for the Inquiry

2.1 The GDPR is the legal regime covering the processing of personal data in the European Union. As a regulation, the GDPR is directly applicable in EU member states. The GDPR is given further effect in Irish law by the 2018 Act. As stated above, the Inquiry was commenced pursuant to section 110 of the 2018 Act. By way of background in this regard, under Part 6 of the 2018 Act, the DPC has the power to commence an inquiry on several bases, including on foot of a complaint, or of its own volition.

2.2 Section 110(1) of the 2018 Act provides that the DPC may, for the purpose of section 109(5)(e) or section 113(2) of the 2018 Act, or of its own volition, cause such inquiry as it thinks fit to be conducted, in order to ascertain whether an infringement has occurred or is occurring of the GDPR or a provision of the 2018 Act, or regulation under the Act, that gives further effect to the GDPR. Section 110(2) of the 2018 Act provides that the DPC may, for the purposes of section 110(1), where it considers it appropriate to do so, cause any of its powers under Chapter 4 of Part 6 of the 2018 Act (excluding section 135 of the 2018 Act) to be exercised and / or cause an investigation under Chapter 5 of Part 6 of the 2018 Act to be carried out.

ii. Data Relationship

2.3 In notifying the personal data breach on 4 March 2021, Fastway initially identified itself as a data controller with the meaning of Article 4(7) of the GDPR.[1] Fastway, then, further clarified in the course of the personal data breach handling process that in some cases it was a controller, in some a joint controller and in some other a processor.[2] As outlined below, the scope of the Inquiry and this Decision relates to the obligation to implement appropriate technical and organisational measures pursuant to 32(1) of the GDPR. This obligation applies equally to data controllers and data processors. Therefore, it is not necessary for the purposes of this Decision to consider for which exact processing Fastway is a controller, joint controller, or processor. Fastway has identified itself as either a controller or processor in respect of all of the relevant processing operations under consideration in this Decision. Therefore, the obligation under 32(1) of the GDPR applies to Fastway in all of those circumstances.

iii. Legal Basis for the Decision

2.4 Section 111 of the 2018 Act requires that the DPC must consider the information obtained during the Inquiry to decide whether an infringement is occurring or has occurred and, if so, to decide on the corrective powers, if any, to be exercised. As the sole member of the DPC as defined in section 15 of the 2018 Act, I perform this function in my role as the decision-maker in the DPC. In so doing, I am required to assess all of the materials and submissions gathered during the Inquiry, as well as submissions that Fastway has furnished to me, and any other materials which I consider to be relevant in the course of the preparation of this Decision.

2.5 On 11 April 2022 I issued a Draft Decision to Fastway. Fastway made submissions on the Draft Decisions on 9 and 25 May 2022.

2.6 Having considered the submissions that Fastway decided to make in respect of the Draft Decision on 9 and 25 May 2022, I had regard to those submissions before proceeding to make this Decision under section 111 of the 2018 Act.

3. Factual Background

3.1 Fastway is a company limited by shares[3], which provides courier services, such as delivery of parcels, letters, packages, and documents, as well as parcel tracking and tracing options.

[1] Personal Data Breach Notification, dated 4 March 2021, page 1.
[2] Update Personal Data Breach Notification, dated 10 March 2021.
[3] It appears that A&G Couriers Limited T/A Fastway Couriers (Ireland) is a registered company limited by shares, CRO no. 339340.

It appears to be "*one of the largest courier businesses in Ireland, handling over 25 million parcels annually, as the delivery partner to over 15,000 Domestic and International clients*"[4].

3.2 Fastway processes personal data of data subjects related to each parcel in order deliver them, and stores these personal data in its internal report system [redacted] for a period of thirty (30) days. After this period, the personal data is anonymised[5].

3.3 Fastway notified the DPC of the personal data breach on 4 March 2021.[6] The personal data breach notification concerned what Fastway described as a cyber-attack[7] which resulted in unauthorised access to personal data held by Fastway. Fastway had engaged its service provider IT Software Contractor ("**IT Service Provider A**") to undertake a "Brexit project" to provide Revenue & Customs with access to the internal reporting system [redacted] to facilitate declarations of duty and VAT.[8] To facilitate this work Fastway "*requested for a developer [IT Service Provider A] to immediately facilitate access to the* [redacted] *reports for external review*".[9] IT Service Provider A made system changes and, during this work, the server on which [redacted] rests became exposed to the public internet. It is suggested by Fastway that due to insufficient checks on security patches, user restrictions and access controls by the developer, the configuration of the affected server was done incorrectly, and the IP address of the affected server was inadvertently exposed following the implementation of the systems changes.[10]

3.4 The notified personal data breach occurred when an individual gained access to the exposed server and exfiltrated personal information pertaining to a large number of data subjects.

3.5 The personal data breach notification indicated that 446,143 data subjects were affected by the incident[11] and that their names, home addresses, email addresses and mobile numbers were disclosed.[12] Fastway further clarified that these categories of personal data might not be fully present in each record affected by the personal data breach, since the data collected is client specific[13] and not all fields are mandatory.[14] Fastway also indicated

---

[4] "About Us" page at Fastway website https://fastway.ie/why-fastway/about-us/ (last access) 7 March 2022.
[5] Personal Data Breach Notification, dated 4 March 2021, page 2-3.
[6] Personal Data Breach Notification, dated 4 March 2021.
[7] In response to the "Nature of breach" in the Personal Data Breach Notification Form Fastway replied "Hacking", cfr. Personal Data Breach Notification, dated 4 March 2021, page 2.
[8] Personal Data Breach Notification, dated 4 March 2021, page 2.
[9] Data Breach Report, page 5.
[10] Data Breach Report, page 6.
[11] Personal Data Breach Notification, dated 4 March 2021, page 3.
[12] Personal Data Breach Notification, dated 4 March 2021, page 3; as further specified in Fastway response to queries, dated 18 March 2021, page 7-8.
[13] Fastway clarified that "*the term 'client' is used to describe the businesses who use Fastway's services as a "last mile" parcel delivery service to those businesses' 'customers'. Fastway's clients provide us with certain personal data of customers required to make deliveries to those customers.*", cfr., in Fastway response to queries, dated 18 March 2021, page 8.
[14] Fastway clarified "*In other words, the customer data provided by clients differs depending on the client. For example, some clients do not provide Fastway with customers' telephone numbers or email addresses. Therefore, the categories of data at A-E above is the full extent of personal data which was compromised in respect of each data subject and, in relation, to some*

that there were a further 602,430 data subjects whose data was anonymised, and therefore these records were unintelligible.[15] Finally, Fastway stated that 624 couriers were also affected by the personal data breach, however in this case the personal data was limited to couriers' names.[16]

3.6 Fastway further clarified that the identified 446,143 data subjects referred to *"unique data subjects whose data was not anonymised"*, since in some cases data subjects had multiple parcels from multiple Fastway clients.[17] In its Submissions on the Commencement Letter (the '**Submissions on the Commencement Letter**'), Fastway explained:

> *"as around 10 000 records were accessed, and we are still unable to determine which of the 446 143 records these comprised. We are also still unable to determine how many duplicates may have been contained within the file the intruder accessed, therefore the total number of data subjects within the file may be less as there can be around 5 transactional records per data subject."*[18]

3.7 In its Additional Submissions on the Draft Decision (the "**Additional Submissions on the Draft Decision**") dated 25 May 2022, Fastway made submissions regarding the number of data subject *"actually accessed"*:

> *"Although the data of 446,143 data subjects was potentially at risk, it is important to emphasise that only the records of 10,000 data subjects were actually accessed. Accordingly, it is Fastway's view that only the data of these 10,000 data subjects that should be taken into account when considering a potential administrative fine pursuant to Article 83(2)(a)."*[19]

3.8 With reference to its "Brexit project", Fastway stated that this project was *"properly mapped and planned in accordance with the Fastway Project Process"*[20], providing the DPC with the related emails exchange between Fastway and IT Service Provider A on 19 and 20 January 2021.[21] Nonetheless, on 7 February 2021 this project became *"super urgent"* as indicated by the emails provided by Fastway.[22] In that regard, the DPC wishes to underline

---

data subjects, it would not have been all categories from A-E but a lesser subset.", cfr., in Fastway response to queries, dated 18 March 2021, page 8.

[15] Update Personal Data Breach Notification, dated 5 March 2021, page 1.

[16] Fastway response to queries, dated 18 March 2021, page 9.

[17] Fastway response to queries, dated 18 March 2021, page 8.

[18] Fastway Submissions on the Commencement Letter and related attachments, dated 8 November 2021, page 1.

[19] Fastway Additional Submission on the Draft Decision, dated 25 May 2022, page 1.

[20] Fastway Submissions on the Commencement Letter and related attachments, dated 8 November 2021, page 8. In its Submissions on the Draft Decision, dated 9 May 2022, Fastway clarified that: *"the "Brexit project" was an ongoing matter lasting over a year, and that the revenue reporting access was only one of the project deliverables. When the data incident was reported to your offices, and in subsequent correspondence, an attempt was made to isolate this particular deliverable (ie the "Brexit Project"), which may have resulted in some confusion."* in Fastway Submissions on the Draft Decision, dated 9 May 2022, page 2.

[21] D.1. 2021-01-19 Email – Between Fastway and Devteam.

[22] D.4. 2021-02-07 Email – Fastway and Devteam – Scoping. In particular, in the email it is reported: *"Any questions let me know, but this work is super urgent so if needs be and we need to consider a workaround if it was to take longer than expected then let me know. I want to get this groomed and estimate provided to Revenue Monday morning. As we can see there are*

that it appears to be a discrepancy in the timeline description provided by Fastway: although the emails provided show that IT Service Provider A was requested to undertake the system changes on 7 February 2021, Fastway indicated in its previous submission that it made the request to IT Service Provider A on 10 February 2021.[23]

3.9 In configuring the changes on the system, on 23 February 2021 (approximately 9am) the server became exposed to public access.[24]

3.10 Fastway outlined that it became aware of the personal data breach on 24 February 2021[25] when an email was received by members of Fastway Franchise Support Office from an individual claiming to have gained access to an exposed server.[26] This email was initially thought to be a phishing email and it was forwarded to IT Service Provider A for investigation on 25 February 2021.[27] On 26 February 2021 IT Service Provider A brought all access and permissions to the server under surveillance,[28] and ended the vulnerability at approximately 9am.[29]

3.11 An information security consultancy firm, prepared a report on the incident (the "**IT Security Report**") for Fastway. This report stated that Fastway's system was exposed from approximately 9am on 23 February 2021 to approximately 9am on 26 February 2021.[30] In this period of time, Fastway identified that an unauthorised individual had gained access on the 24 February 2021 at 07:18[31] and successfully downloaded [redacted] the personal information of data subjects in [redacted] format.[32] Fastway also observed that it did not experience any loss of personal data, although it could not be certain whether or not the unauthorised individual had destroyed the data following its exfiltration.[33] In its Submissions on the Draft Decision (the "**Submissions on the Draft Decision**") dated 9 May 2022, Fastway also added that it *"contracted an external company to conduct a deepweb search to identify if any data accessed during this incident had been leaked. The results came back in the negative."*[34]

---

changes not just with reporting but also SPE. I have added [IT Service Provider A] as they might get a chance to look at this early and then you can take your discussion."

[23] Fastway response to queries, dated 18 March 2021, page 1.

[24] Fastway response to queries, dated 18 March 2021, page 2. This is also confirmed by the external information security consultancy firm, consulted by Fastway, cfr. IT Security Report, page 9.

[25] Personal Data Breach Notification, dated 4 March 2021, page 2.

[26] Fastway response to queries, dated 18 March 2021, page 1.

[27] Fastway response to queries, dated 18 March 2021, page 1.

[28] Fastway response to queries, dated 18 March 2021, page 1.

[29] Data Breach Report, page 5. This is also confirmed by the external information security consultancy firm, consulted by Fastway, cfr. IT Security Report, page 10.

[30] IT Security Report, page 9-10.

[31] Fastway response to queries, dated 18 March 2021, page 1 and 14. This is also confirmed by the external information security consultancy firm, consulted by Fastway, cfr. IT Security Report, in particular: *"The analysis of the provided log files showed that IP address [redacted] was exposed from the 9am on the morning of the 23rd of February and 6am on the morning of the 26th of February. During this time, the IP address [redacted] was accessed by approximately 21 IP addresses across eight countries. All but one of the IPs were scanning and did not access the data. Only one access to the [redacted] on the server could be identified in the logs"*, page 5.

[32] Data Breach Report, page 5.

[33] Personal Data Breach Notification, dated 4 March 2021, page 4.

[34] Fastway Submissions on the Draft Decision, dated 9 May 2022, page 6.

3.12 On 2 March 2021, IT Service Provider A confirmed Fastway had been breached and personal data was compromised.[35] Consequently, Fastway initiated the Incident Management Plan, which included investigating the event and timeline, as well as preparing the personal data breach notification to the DPC.[36]

3.13 After the initial personal data breach notification to the DPC on 4 March 2021, Fastway provided updates on the personal data breach notification to the DPC on 5 March 2021[37] and 10 March 2021[38]. On 5 March 2021, Fastway also reported the incident to the An Garda Síochána.[39] Fastway also notified the personal data breach to its clients and 265,742 data subjects were notified by Fastway on behalf of its clients.[40] Fastway also prepared an interim incident report ('**Data Breach Report**') on 5 March 2021[41] and engaged with an external information security consultancy firm to prepare a full incident response to the personal data breach.[42] Furthermore, on 11 March 2021, Fastway published a public statement on its website.[43]

3.14 The DPC raised queries with Fastway on 5 March 2021[44] to which Fastway responded on 18 March 2021.[45] In its response to the queries dated 18 March 2021, Fastway indicated that investigative work carried out by IT Service Provider A confirmed that a breach of personal data had occurred. The response also contained a number of documents in relation to the circumstances of the personal data breach.[46]

3.15 On 12 March 2021, the DPC requested the clients list.[47] Fastway did not provide the clients list to the DPC. On 19 March 2021, the DPC issued a letter to Fastway regarding the nature of the personal data breach and the related obligations of communication of a personal data breach to data subjects.[48] On 31 March 2021, the DPC received a response to its letter by the legal representatives of Fastway clarifying the use of the word "cyber-attack" and the ongoing investigation by the An Garda Síochána.[49]

---

[35] Fastway response to queries, dated 18 March 2021, page 2.
[36] Fastway response to queries, dated 18 March 2021, page 2-3.
[37] Update Personal Data Breach Notification, dated 5 March 2021.
[38] Update Personal Data Breach Notification, dated 10 March 2021.
[39] Fastway response to queries, dated 18 March 2021, page 7.
[40] Fastway response to queries, dated 18 March 2021, page 8-9.
[41] Data Breach Report.
[42] Fastway response to queries, dated 18 March 2021, page 6.
[43] Fastway response to queries, dated 18 March 2021, page 9.
[44] DPC queries, dated 5 March 2021.
[45] Fastway response to queries, dated 18 March 2021.
[46] Data Security Incident Management Procedure; Data Breach Report; Client notification; Client update; Customer notification; Emails with hacker.
[47] DPC request for client list, dated 12 March 2021.
[48] DPC letter to Fastway, dated 19 March 2021.
[49] Letter from legal representatives on behalf of Fastway, dated 31 March 2021.

3.16 On 23 March 2021, the DPC requested the IT Security Report[50] and on 30 March 2021 the DPC requested Fastway's record of processing activities.[51] On 2 April 2021, Fastway provided the record of processing.[52] On 6 April 2021, the DPC further requested the IT Security Report[53], which was provided by Fastway on the same day.[54]

3.17 On 6 May 2021, the DPC raised further queries with Fastway.[55] Fastway provided a response on 17 May 2021, and also provided the audit questionnaire template related to IT Service Provider A.[56]

3.18 On 25 May 2021, the DPC raised further queries with Fastway.[57] Fastway provided a response on 27 May 2021.[58]

3.19 The DPC issued an Inquiry Commencement Letter ('**the Commencement Letter**') via registered post to Fastway on 18 October 2021 notifying Fastway that the DPC had commenced an Inquiry under and in accordance with section 110(1) of the 2018 Act.[59] The letter contained details of the personal data breach notified to the DPC which would be the subject of the Inquiry and contained six questions seeking further information from Fastway.

3.20 The decision to commence the Inquiry was taken having regard to the circumstances of personal data breach notified by Fastway. The Commencement Letter informed Fastway that the Inquiry would examine whether or not Fastway discharged its obligations in connection with the subject matter of that personal data breach and determine whether or not any provision(s) of the 2018 Act and/or the GDPR had been contravened by Fastway in that context. In this regard, the scope of the Inquiry was expressly stated to focus on Fastway's organisational and technical measures in place to ensure appropriate security of the personal data pursuant to Article 32(1) of the GDPR in the context of its processing of personal data in respect of its provision of delivery services and its storage of personal data in its internal report system [redacted] at the time of the notified personal data breach.

3.21 The Commencement Letter set out that the Inquiry would formally document the facts as they relate to the subject of the Inquiry. The facts, as established during the course of the Inquiry, are set out in this Decision.

3.22 Fastway provided submissions in response to the Commencement Letter on 8 November 2021.[60] In its submissions, Fastway provided extensive documentation on technical and

[50] DPC Request for the external IT Security Report, dated 23 March 2021.
[51] DPC Request for Record of Processing Activities, dated 30 March 2021.
[52] Fastway response, dated 2 April 2021 and Fastway Record of Processing Activities.
[53] DPC Further request for the external IT Security Report, dated 6 April 2021.
[54] IT Security Report, provided on 6 April 2021.
[55] DPC further queries, dated 6 May 2021.
[56] Fastway response to further queries, dated 17 May 2021 and Fastway Audit questionnaire template.
[57] DPC further queries of clarification, dated 25 May 2021.
[58] Fastway response to further queries of clarification, dated 27 May 2021.
[59] DPC Inquiry Commencement Letter, dated 18 October 2021.
[60] Fastway Submissions on the Commencement Letter and related attachments, dated 8 November 2021.

organisational measures which Fastway had in place to meet the requirements of the GDPR.

3.23 Having received Fastway's submissions, the DPC proceeded to prepare the Draft Decision. On 11 April 2022 I provided the Draft Decision to Fastway. Fastway was afforded the opportunity to make submissions on the proposed infringement that was provisionally identified in the Draft Decision and the corrective powers that I proposed to exercise. On 9 and 25 May 2022 Fastway made submissions on the Draft Decision. I have had full regard to those submissions and I have reached conclusions that an infringement of data protection legislation has occurred and that it is necessary to exercise certain corrective powers. This infringement and corrective powers are set out in this Decision.

4. Scope of the Inquiry

4.1 The scope of the Inquiry, which was set out in the Inquiry Commencement Letter, was to examine whether or not Fastway discharged its obligations in connection with the subject matter of the personal data breach and to determine whether or not any provision(s) of the 2018 Act and/or the GDPR have been contravened by Fastway in that context.

4.2 In this regard, the Commencement Letter specified that the Inquiry would focus on Fastway's organisational and technical measures in place to ensure security of the personal data in the context of its processing of personal data in respect of its provision of delivery services and its storage of personal data in its internal report system [redacted] at the time of the notified personal data breach. In particular, the Commencement Letter expressly stated that the scope of the Inquiry would include Article 32(1) of the GDPR. The Commencement Letter stated that the Inquiry would focus on the areas of Security of Personal Data, Data Protection Governance, and Training and Awareness.

5. Issue for Determination

5.1 Having considered the Commencement Letter, and the other relevant materials, I find that it falls for me to consider in this Decision whether Fastway has complied with its obligations under Article 32(1) of the GDPR by implementing appropriate technical and organisational measures to ensure appropriate security of the personal data in the context of its processing of personal data in respect of its provision of delivery services and its storage of personal data in its internal report system [redacted] at the time of the notified personal data breach.

6. Issue: Article 32(1) of the GDPR

6.1 Article 32(1) of the GDPR details the security obligations for the processing of personal data by controllers and processors and sets out criteria for assessing what constitutes *'appropriate security'* and *'appropriate technical or organisational measures':*

> *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.*

6.2 Recital 83 of the GDPR provides useful interpretative indications on how to assess data security risk:

> *"In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage."*

i. Assessing Risk

6.3 Article 32(1) of the GDPR obliges controllers and processors to implement a level of security appropriate to the risks presented by its processing of personal data.

6.4 The level of security must be appropriate to the risk presented to the rights and freedoms of natural persons, and must have regard to the state of the art, the costs of

implementation and the nature, scope, context and purposes of processing. Therefore, the first step is to assess the risk presented to the rights and freedoms of data subjects by the processing of personal data (as assessed below), and then to assess the appropriateness of the security measures implemented (as detailed in the following Parts 6.ii and 6.iii).

6.5 Recital 76 of the GDPR provides further guidance as to how risk should be evaluated:

> *The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.*

6.6 *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources and others* judgement[61] provides further guidance on this risk assessment. In this case, the Court of Justice of the European Union ("**the CJEU**") declared the Data Retention Directive[62] invalid. The Directive required electronic communication service providers to retain certain data for a period of time. The CJEU held that the Directive did not ensure effective protection of the data retained against the risk of abuse and unlawful access in circumstances where it did not lay down specific rules in relation to

> *(i) the vast quantity of data whose retention is required by that directive, (ii) the sensitive nature of that data and (iii) the risk of unlawful access to that data, rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality.*[63]

6.7 Therefore, risk must be assessed objectively by reference to (i) the likelihood of the risk to the rights and freedoms of natural persons, and (ii) the severity of that risk.

6.8 Hence, the risk assessment must consider, first, the likelihood of the risk to the rights and freedom of data subjects whose personal data are processed by Fastway; and second, the severity of that risk in respect of the rights and freedoms of the data subjects. These objective assessments must be made by reference to the nature, scope, context and purposes of the processing. In considering these factors, regard must also be had to the quantity of personal data processed and the sensitivity of that data. Only in light of the risk assessment is possible to analyse the appropriateness of the security measures implemented (as detailed in the following Parts 6.ii and 6.iii).

---

[61] Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General, intervener: Irish Human Rights Commission, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others*, judgment of 8 April 2014 (ECLI:EU:C:2014:238).

[62] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

[63] Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd, op. cit,* para 66.

6.9 Therefore, it is necessary first to examine the nature, scope, context and purposes of the processing. In terms of the nature of the Fastway's processing of personal data, this consists of electronic records stored in Fastway's server [redacted] for a period of thirty (30) days. After this period, the personal data is anonymised[64]. In respect of each data subject, Fastway may process personal data such as names, home addresses, email addresses and mobile numbers. However, Fastway clarified that that these categories of personal data might not be fully present in each record, since the data collected depends on its clients and not all fields are mandatory.[65] In these circumstances, the personal data processed by Fastway may be considered at the lower end of the scale in terms of sensitivity. Nonetheless, the quantity of personal data processed by Fastway is significant: in its Additional Submissions on the Draft Decision, Fastway reported that "*the records of 10,000 data subjects were actually accessed*".[66]

6.10 The scope and the context of the processing of the personal data involves the use of package recipient address and contact information to facilitate the delivery of packages and, potentially, revenue and sender reconciliation records.

6.11 The purposes of Fastway's processing of personal data relates to Fastway's delivery service. In its Record of Processing, Fastway identified five purposes: Custom declaration, Manifesting, Manifest enhancement, Scan event capture – tracking, Delivery performance reporting (used internally and for clients).[67]

6.12 Assessed objectively, I consider that the risks posed by Fastway's processing at the time of the personal data breach involved low to moderate risks both in likelihood and severity to the rights and freedoms of data subjects. Although the significant quantity of personal data related to a large number of data subjects processed and stored for a period of thirty (30) days by Fastway, this personal data may be considered at the lower end of the scale in terms of sensitivity. Therefore, I find that the severity of the risk to the rights and freedoms of natural persons is low. The likelihood of the risk relates to the possibility that such large quantity of personal data, stored as electronic records in a server of Fastway's IT infrastructure, may be subjected to an accidental or unlawful destruction, loss, alternation, unauthorised disclosure or access to personal data. In its Submissions on the Draft Decision, Fastway provided an overall description and related documentation on the

[64] Personal Data Breach Notification, dated 4 March 2021, page 2-3.
[65] Fastway clarified "*In other words, the customer data provided by clients differs depending on the client. For example, some clients do not provide Fastway with customers' telephone numbers or email addresses. Therefore, the categories of data at A-E above is the full extent of personal data which was compromised in respect of each data subject and, in relation, to some data subjects, it would not have been all categories from A-E but a lesser subset.*", cfr., in Fastway response to queries, dated 18 March 2021, page 8.
[66] Fastway Additional Submission on the Draft Decision, dated 25 May 2022, page 1.
[67] In Fastway's Record of Processing there are identified six purposes, however one purpose (Delivery performance reporting) is reported twice with reference to two different categories of personal data: on one instance this purpose refers to the categories of personal data of name, address, label number, email address, telephone number of "client customers"; on a second instance this purpose is related to the name of couriers; cfr. Fastway Record of Processing Activities.

systems and controls implemented to ensure data security prior to the personal data breach in 2020, stating that

> *"The position at this stage was that risks to the data subjects' rights and freedoms were not determined as being high, not only in terms of the nature of the personal data processed, but also as a result of the already implemented security measures."*[68]

6.13 However, pursuant to Article 32(1)(d) of the GDPR and in light of the obligation to regularly evaluate the effectiveness of technical and organisational measures, it is clear that Fastway should have conducted a risk assessment before initiating the process of reviewing access to its internal server in the context of the "Brexit project" in order to identify any possible risk arising from this specific change to the system. Its failure to do so aggravating the likelihood regarding the risks to the rights and freedoms of data subjects. Fastway confirmed that the risk assessment regarding the changes to the system was not performed.[69] Therefore, I consider that there was a moderate likelihood regarding the risks to the rights and freedoms of data subjects. In the Data Breach Report, in evaluating the circumstances around the personal data breach, Fastway identified various critical aspects, among of them:

> *"Process review 3: A Risk Assessment should have been conducted to carry out vulnerability identification, to review and address any changes or new risks in data protection by the way of security gap analysis.*
> *- Process review 4: During the risk assessment, the* [redacted] *architectural issue and vulnerability could have been caught. All aspects should have been considered from data storage, remote access for other stakeholders and verify if the policies and procedures are adequate."*[70]

6.14 Fastway explained that a possible reason for the lack of the risk assessment prior to the changes to the system was due to an *"urgent request to facilitate declarations of duty and VAT"*.[71] However, Fastway also correctly recognised that urgency cannot allow exceptions to the obligation to implement appropriate security measures and to follow policies and procedures that have been implemented[72].

---

[68] Fastway Submissions on the Draft Decision, dated 9 May 2022, page 7, see also Data Flows Mapping, dated 13 August 2020; and Personal Data Flow.

[69] In the personal data breach notification, to the query on *"What deficiencies in these organisational or technical measures have been identified as a result of this breach"* Fastway reported: *"Security review by security lead and approval. Risk assessment process as part of security and data protection. Staff training as identified. Security Audits. Vulnerability compliance tools"*, cfr. Personal Data Breach Notification, dated 4 March 2021, page 3. The lack of risk assessment prior to the "Breixt Project" was also confirmed in Fastway Submissions on the Draft Decision, dated 9 May 2022, page 3, point no 10; page 8 and page 11.

[70] Data Breach Report, page 9.

[71] Personal Data Breach Notification, dated 4 March 2021, page 2.

[72] Fastway identified, as another aspect related to the circumstances of the personal data breach, that *"Process review 2: urgency of the any task can never be allowed ignore following the process."*, cfr. Data Breach Report, page 9.

6.15 In all the circumstances, I consider that the likelihood and the severity of the risk to the rights and freedoms of the data subjects was low to moderate and Fastway did not assess the risks before the decision to apply the changes on its system.

ii. Security Measures Implemented by Fastway

6.16 Fastway detailed the technical and organisational measures that it had in place before the personal data breach, at the time of the personal data breach and the measures it consequently adopted immediately after the personal data breach. For the avoidance of doubt, this Decision does not consider the appropriateness of the level of security that Fastway currently implements but rather considers the measures in place at the time of the personal data breach (23 February 2021) and specifically regarding its processing of personal data in respect of its provision of delivery services and its storage of personal data in its internal report system [redacted], which became exposed to the public internet during the implementation of the "Brexit project".

6.17 The measures relevant to Fastway's processing of personal data can be categorised as:

a) IT Infrastructure and technical measures;
b) Data Protection Policies and Procedures, and Training

a) IT Infrastructure and technical measures

6.18 Fastway processes personal data of data subjects related to each parcel in order to make deliveries, and it stores these personal data in its internal report system [redacted] for a period of thirty (30) days on one of its servers. After this period, the personal data is anonymised[73]. This personal information is stored in [redacted][74] Before the personal data breach, this information was not encrypted.[75] The internal reporting system was not publicly available; however Fastway underlined that security controls were limited to internal access control procedures and these security controls were not the same as those existing in Fastway external facing applications. In this regard, Fastway reported as identified deficiencies of technical and organisational measures as follows:

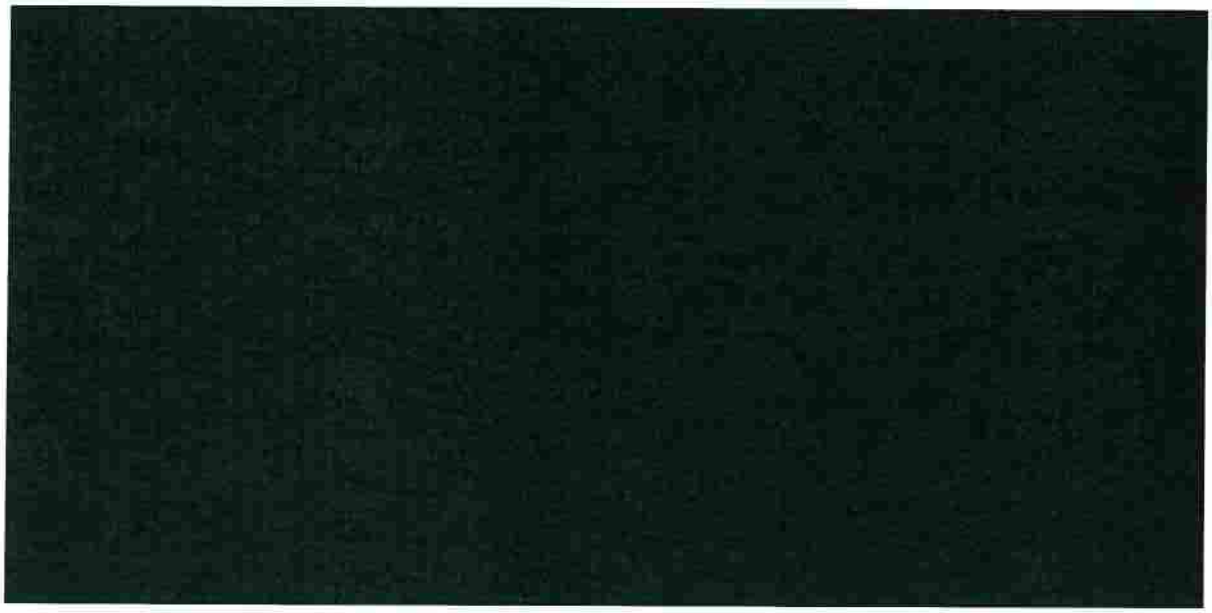
> *"Our internal reporting system are never publicly available – internal access procedures were only considered necessary in this respect, this was clearly a grave oversight. Irrespective of a system being considered internal, it should be subject to the same security controls as all our existing external facing applications. Failure to*

[73] Personal Data Breach Notification, dated 4 March 2021, page 2-3.
[74] Data Breach Report, page 5.
[75] Fastway stated: *"At the time of our data breach the [redacted] table was not encrypted, this is what led to the exploitation of the vulnerability. This has been remedied since then."*cfr. Fastway response to further queries, dated 17 May 2021, page 2.

follow existing process and security protocols, perceived time constraints, and instruction without approval from the appropriate person lead to the breach".[76]

6.19 Fastway provided a representation of the IT infrastructure before the system changes (figure no. 1), where the [redacted] was not public:

[redacted]



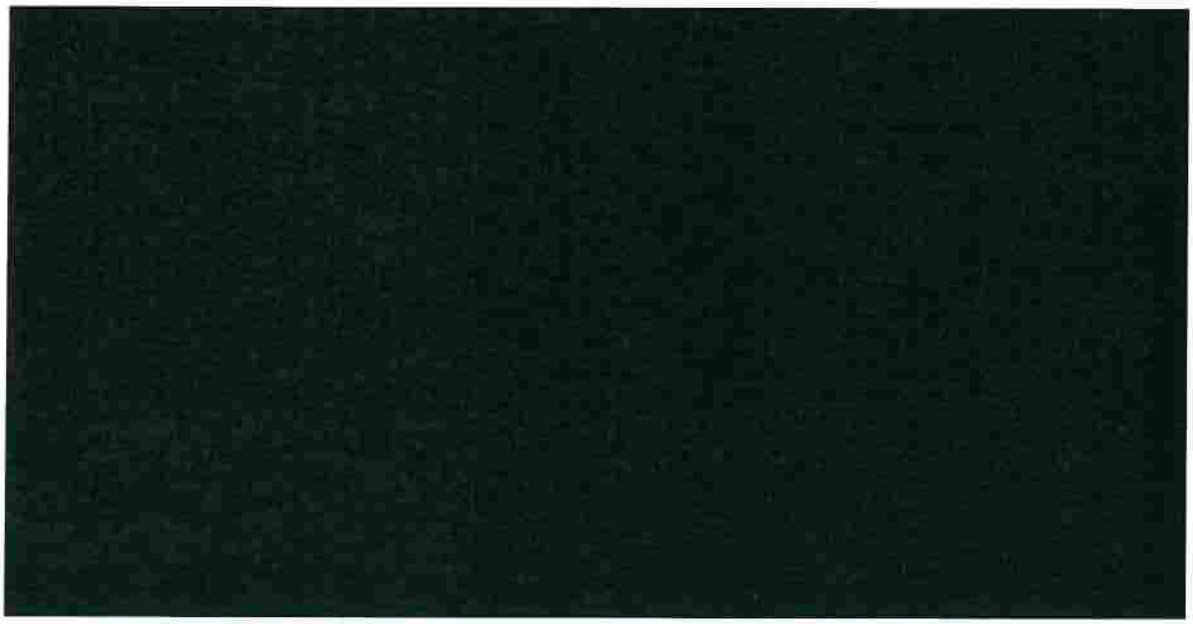
6.20 In its Submissions on the Draft Decision, Fastway clarified that the "Brexit project" was "*an ongoing matter lasting over a year*".[78] The revenue reporting access (the one involved in the personal data breach, as further described below) was only one of the project deliverables and for this project deliverable Fastway agreed a Statement of Work (the "**Statement of Work**") with the IT Service Provider A on 27 January 2021.[79]

6.21 On 7 February 2021, Fastway requested IT Service Provider A to undertake the "Brexit project"[80], consisting of allowing Revenue Commissioners and Customs access to Fastway's internal reporting system [redacted] to facilitate declarations of duty and VAT.[81] In doing so, Fastway was under an obligation to implement appropriate organisational and technical measures to ensure a level of security appropriate to the risk. This section details the technical measures implemented, while the following section details the organisational measures implemented.

[76] Personal Data Breach Notification, dated 4 March 2021, page 3.
[77] Data Breach Report, page 7.
[78] Fastway Submissions on the Draft Decision, dated 9 May 2022, page 2, point no 4.
[79] Fastway Submissions on the Draft Decision, dated 9 May 2022, page 2, point no 6.
[80] D.4. 2021-02-07 Email – Fastway and Devteam – Scoping.
[81] Data Breach Report, page 5.

6.22 IT Service Provider A was requested to configure [redacted] to grant access to the internal reporting system [redacted].[82] Fastway reported that, in making these system changes, IT Service Provider A incorrectly exposed the IP publicly, including an open port.[83] Fastway provided a representation of the infrastructure after the new configuration (figure no. 2), where the [redacted] was made public and the [redacted] was added without security:

[redacted]



6.23 Fastway stated that IT Service Provider A did not check and complete the necessary security patches nor review user restrictions and access control before exposing the IP publicly.[85] Fastway further clarified that:

> *"The system was configured to authenticate requests to the [redacted] instance using a [redacted] and due to incorrect configuration this triggered the incident that exposed the data."*[86]

In its Submissions on the Draft Decision, Fastway further clarified that:

> *"reference to the "security patch" did not allude to a patch which should have been updated prior to the project, but rather to the vulnerability being "patched" or addressed.*
> *It was therefore not the vulnerability of the software which was the issue, rather, the vulnerability arose due to the incorrect configuration by the developer."*[87]

[82] Personal Data Breach Notification, dated 4 March 2021, page 2.
[83] Personal Data Breach Notification, dated 4 March 2021, page 2.
[84] Data Breach Report, page 7.
[85] Personal Data Breach Notification, dated 4 March 2021, page 2.
[86] Data Breach Report, page 6.
[87] Fastway Submissions on the Draft Decision, dated 9 May 2022, page 8.

6.24 Fastway briefly explained the issues that arose from such misconfiguration as:

> *"Issues identified:*
> *1. [redacted] was misconfigured to be open.*
> *2. [redacted] was configured but the [redacted] was not closed.*
> *3. [redacted] that was provided by [redacted] for user restriction was not applied. By default the [redacted] was operational for only one user and later on [redacted] released the [redacted]."*[88]

6.25 As reported in Part 3, Fastway's system was exposed from approximately 9am on 23 February 2021 to approximately 9am on 26 February 2021,[89] during which an unauthorised individual gained access on 24 February 2021 at 07:18[90] and successfully downloaded the personal data stored there.[91]

6.26 Fastway summarised the cause of what led to the personal data breach as follows:

> *"The developer should have checked and completed the configuration correctly, the necessary security patches and reviewed user restrictions and access control before exposing the IP publicly."*[92]

6.27 The IT Security Report identified that the root cause of the personal data breach was human error and stated:

> *"It was reported that Fastway have development and security policies in place but that these were not followed.*
> *The IT services company misconfigured the system, which caused the data to be open to the internet. This in turn allowed the intruder to access the data."*[93]

6.28 The IT Security Report further analysed that:

1. *"All changes on production systems should be managed by a Change policy/procedure, which should include the requirement that the risks in making the change be evaluated.*
2. *It should be enforced that there is separation between production, test and UAT environments and Data.*

---

[88] Fastway response to queries, dated 18 March 2021, pages 3-4.
[89] IT Security Report, page 9-10.
[90] Fastway response to queries, dated 18 March 2021, page 1 and 14. This is also confirmed by the external information security consultancy firm, consulted by Fastway, cfr. IT Security Report, in particular: *"The analysis of the provided log files showed that IP address [redacted] was exposed from the 9am on the morning of the 23rd of February and 6am on the morning of the 26th of February. During this time, the IP address [redacted] was accessed by approximately 21 IP addresses across eight countries. All but one of the IPs were scanning and did not access the data. Only one access to the [redacted] on the server could be identified in the logs"*, page 5.
[91] Data Breach Report, page 5.
[92] Data Breach Report, page 6.
[93] IT Security Report, page 10.

3. *All change on production systems should be carried out by appropriately Qualified/experienced persons.*
4. *A penetration test of the Fastway perimeter should be carried out to ensure there are no other similar issues.*
5. *There should be a separation of duties so that persons involved in development are not involved in day-to-day operations or system administration activities."*[94]

6.29 On 26 February 2021, IT Service Provider A brought all access and permissions of the server under surveillance,[95] and ended the vulnerability at approximately 9am.[96] In particular, Fastway reported the following steps taken by IT Service Provider A immediately after the personal data breach:

> *"a. Blocked the [redacted] that was vulnerable. Also, user authentication enabled for [redacted] service listening [redacted] that was comprised will no longer will be available until the user has permission to the same.*
> *b. [redacted] restricted based on Authentication and FTP allowed for particular security group.*
> *c. Security Patch Applied for user restrictions in the [redacted] server.*
> *d. Surveyed the damage, Filtered the traffic, Isolated the system under compromise.*
> *e. All access credentials and permissions brought under surveillance for various roles and users in the network.*
> *f. Configure [redacted] to allow [redacted] range and deny everything else.*
> *g. Installed Network Vulnerability monitoring tools.*
> *h. Installed new [redacted] instance and configured.*
> *i. [redacted] Server authorisation restrictions implemented.*
> *j. Improving the existing Infosec policy and planning for introducing new processes to make the infrastructure is fool proof from any breach.*
> *k. Installed Vulnerability scanning tools with alert notifications.*
> *l. All Servers - log Monitoring enabled, configured for audit, and pushed to [redacted] [redacted] and [redacted] wherever applicable.*
> *m. Data in [redacted] at rest encrypted. Data in transit using [redacted] access restricted using [redacted] tool and configured read only for other [redacted] also provided with additional protection hiding sensitive data pursuant to Article 4(1) like Name, Mobile Number, email Address, Country and Address."*[97]

6.30 Fastway was informed by IT Service Provider A about the personal data breach on 2 March 2021[98] and trigged the Incident Management Plan on the same day.[99] Consequently, it notified the personal data breach to the DPC on 4 March 2021, identifying the initial

[94] IT Security Report, page 11.
[95] Fastway response to queries, dated 18 March 2021, page 1.
[96] Fastway response to queries, dated 18 March 2021, page 2. This is also confirmed by the external information security consultancy firm, consulted by Fastway, cfr. IT Security Report, page 10.
[97] Fastway response to queries, dated 18 March 2021, page 7.
[98] Fastway response to queries, dated 18 March 2021, page 2.
[99] Fastway response to queries, dated 18 March 2021, page 2.

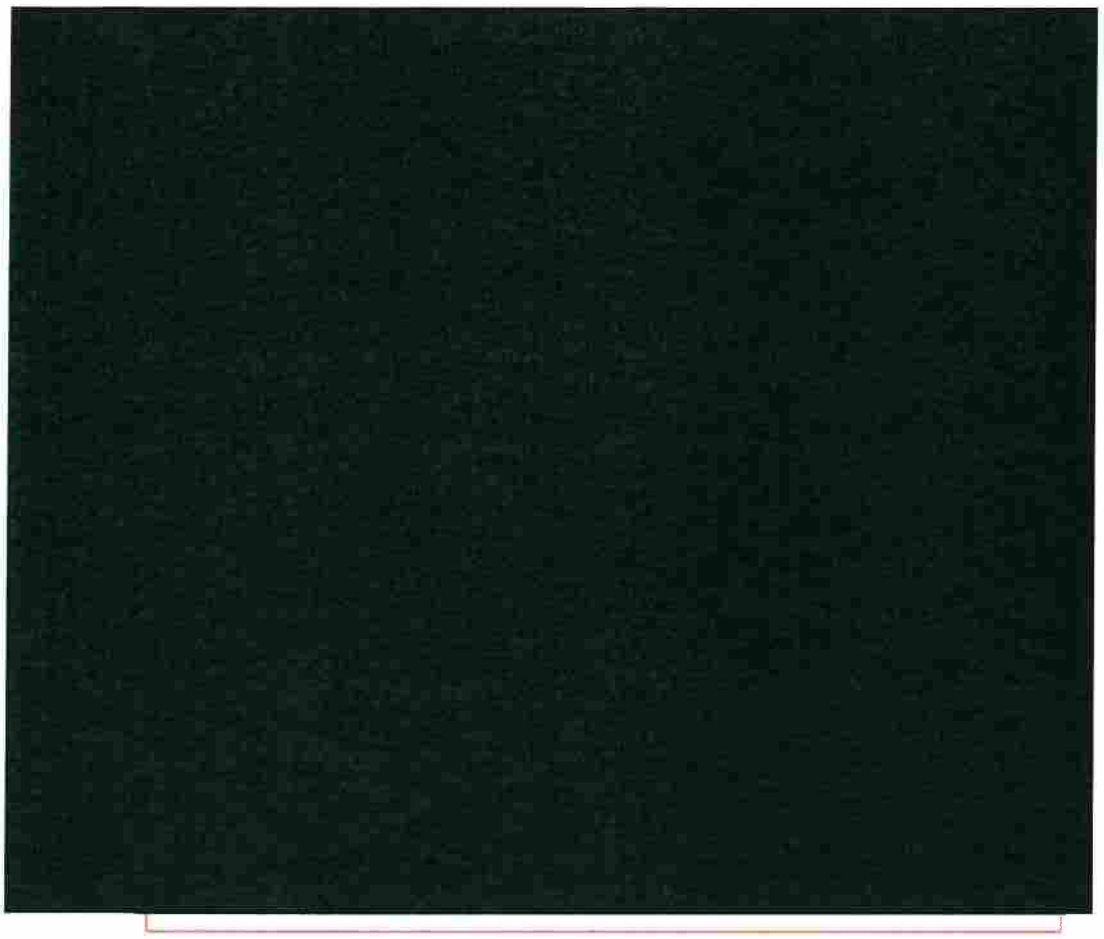
measures taken or proposed to be taken in response to the personal data breach.[100] It appears that a new configuration of its system was completed on 8 March 2021 to replace the compromised one.[101] In particular, Fastway indicated the following actions to prevent the a repetition of the personal data breach:

> *"a. Configure* [redacted] *to allow* [redacted] *range and deny everything else.*
> *b. Installed Network Vulnerability monitoring tools.*
> *c. Installed new* [redacted] *instance and configured.*
> *d.* [redacted] *Server authorisation restrictions implemented.*
> *e. Improving the existing Infosec policy and planning for introducing new processes to make the infrastructure is fool proof from any breach.*
> *f. Installed Vulnerability scanning tools with alert notifications.*
> *g. All Servers - log Monitoring enabled, configured for audit, and pushed to* [redacted] *and* [redacted] *wherever applicable.*
> *h. Data in* [redacted] *at rest encrypted. Data in transit using* [redacted] *access restricted using* [redacted] *tool and configured read only for other* [redacted] *also provided with additional protection hiding personal data pursuant to Article 4(1) like Name, Mobile Number, email Address, Country and Address."*[102]

6.31 Fastway provided a representation of the infrastructure post-breach (figure no. 3):

[100] Personal Data Breach Notification, dated 4 March 2021, page 3-4.
[101] Fastway response to queries, dated 18 March 2021, page 4.
[102] Fastway response to queries, dated 18 March 2021, page 17.

[redacted]



6.32 However, in its Submissions on the Commencement Letter, it appears that Fastway indicated that some measures were ordinarily in place to systematically ensure that systems and servers were configured correctly and, that intrusion detection tools were in the IT Infrastructure:

> *"Solutions used to remotely secure, monitor, manage, and support Fastway endpoints to mitigate risks of data breach incidents, proactive network monitoring, Intrusion detection (using [redacted]) and efficient service delivery include [redacted].*
>
> *We avail use of a checklist configuration settings to guarantee that servers are sufficiently hardened against external attacks. This includes but not limited to;*
>
> *(a) User configuration*
>
> *(b) Network configuration*
>
> *(c) Features and roles configuration (file server, web server)*
>
> *(d) Update installation*
>
> *(e) NTP configuration*
>
> *(f) Firewall configuration*

[103] Fastway response to queries, dated 18 March 2021, page 15.

(g) Remove access configuration
(h) Service configuration
(i) Protect the [redacted] *and other applications*
(j) Logging and monitoring."[104]

6.33 However, given that the stated cause of the personal data breach was partly due to a misconfiguration, it appears that this configuration checklist was not properly implemented, followed and/or effective following the instruction given to IT Service Provider A to implement an immediate change.

6.34 Fastway further specified additional steps it will take to ensure compliance with its obligation to implement appropriate security measures on an ongoing basis, including technical measures such as:

> *"Undertake a full tech stack review of all environments on a regular basis*
> *[...]*
> *Review of the deployment process for software release"*[105].

6.35 At the time of the personal data breach, the personal data stored in the [redacted] was not encrypted and the security controls were not designed having regard to the possibility that the affected data could be viewed by an external entity, as confirmed by Fastway, which stated that the internal reporting system should have been *"subject to the same security controls as all our existing external facing applications"*.[106] Due to the change in the audience to whom the reporting system was exposed to, the new risks associated with such a change ought to have been firstly assessed, as already clarified in above Part 6.i. Accordingly, risk-appropriate measures such as encryption and comprehensive access control procedures should have been implemented before the personal data breach. In that regard, Fastway confirmed that the risk assessment regarding the changes to the systems was not performed,[107] and it failed to implement appropriate mitigating measures.[108]

---

[104] Fastway Submissions on the Commencement Letter and related attachments, dated 8 November 2021, page 4.
[105] Fastway response to queries, dated 18 March 2021, page 18.
[106] In the Personal Data Breach Notification Fastway stated: *"Our internal reporting system are never publicly available – internal access procedures were only considered necessary in this respect, this was clearly a grave oversight. Irrespective of a system being considered internal, it should be subject to the same security controls as all our existing external facing applications. Failure to follow existing process and security protocols, perceived time constraints, and instruction without approval from the appropriate person lead to the breach"*, cfr. Personal Data Breach Notification, dated 4 March 2021, page 3. Furthermore, Fastway stated: *"At the time of our data breach* [redacted] *was not encrypted, this is what led to the exploitation of the vulnerability. This has been remedied since then."*cfr. Fastway response to further queries, dated 17 May 2021, page 2.
[107] In the personal data breach notification, to the query on *"What deficiencies in these organisational or technical measures have been identified as a result of this breach"* Fastway reported: *"Security review by security lead and approval. Risk assessment process as part of security and data protection. Staff training as identified. Security Audits. Vulnerability compliance tools"*, cfr. Personal Data Breach Notification, dated 4 March 2021, page 3.
[108] Data Breach Report, page 9.

6.36 The DPC notes that it appears that in its Submissions on the Draft Decision, Fastway agrees with the above reconstruction contained in the para 6.33, 6.34 and 6.35 and it further underlines the new steps implemented on its system.[109]

6.37 Additionally, certain of Fastway's existing measures, such as the configuration checklist outlined above either do not appear to have been followed, or do not appear to have been effective. Such measures (including encryption and comprehensive access control procedures) could have mitigated or avoided the personal data breach. Considering, then, the way the system changes were conducted from a technical point of view, there was a misconfiguration, which provided unauthorised access to an unknown external entity.[110] This misconfiguration, however, appears partly linked to a failure to follow internal procedures, as further assessed in the next section.

b) Data Protection Policies and Procedures, and Training

6.38 In its submissions during the personal data handling process, Fastway referred to a number of Data Protection Policies and Procedures in place at the time of the personal data breach[111] related to data security and data protection. In its Submissions following the Commencement Letter and the Draft Decision, Fastway provided extensive documentation regarding its Data Protection Policies and Procedures, including training. Although all the provided materials have been considered and assessed by the DPC, as the material scope of this Decision concerns the **measures in place at the time of the personal data breach**, this part of the Decision focuses its analysis on the Data Protection Policies and Procedures, including training, that were in place at that specific point of time (23 February 2021).

6.39 With specific reference to training, Fastway explained it provided various training activities on Data Protection to its personnel before the personal data breach (before 23 February 2021). In particular:

- in October 2018 GDPR training was completed with select staff by external consultant and Fastway further displayed posters at all locations to raise awareness. It also provided Courier Drivers with GDPR awareness material.[112] Furthermore, in its Submissions on the Draft Decision Fastway provided additional

[109] Fastway Submissions on the Draft Decision, dated 9 May 2022, page 9. In particular, Fastway states "*We believe that this goes to the heart of the issue and has been addressed in the change management procedure and the other procedures which have subsequently been implemented*" commenting on para 6.33 above (para 6.31 in the Draft Decision).

[110] IT Security Report stated: "*The root cause of the incident has been found to be misconfiguration and failure to follow policies and procedures by the external IT services company. The security measures taken by the IT services company in this instance were insufficient*", cfr. IT Security Report, page 4.

[111] Fastway reported: "*Failure to follow existing process and security protocols, perceived time constraints, and instruction without approval from the appropriate person lead to the breach*", cfr. Personal Data Breach Notification, dated 4 March 2021, page 3. Further Fastway referred as actions to ensure compliance with security and organisational measures: "*Review information security policies and procedures with a focus on management of third party providers, [...] Review testing of information security processes and procedures including current risks analysis.*", cfr, Fastway response to queries, dated 18 March 2021, page 17-18.

[112] Fastway Submissions on the Commencement Letter and related attachments, dated 8 November 2021, page 6.

emails on the GDPR campaigns and modifications to its website that it made in light of the new regulatory framework;[113]

- in 2019 it engaged with various campaigns (throughout via emails) to promote "Phishing awareness" among its staff;[114]
- in 2020, among the various activities, Regional Franchisees and Courier Franchisees were provided with an updated and practical GDPR compliance manual; standard courier procedures incorporated data protection measures and every "Depot champion" was provided with a GDPR audit checklist to ensure ongoing compliance;[115]
- in February 2021 Data Protection training was provided to all staff and across all Fastway depots.[116]

6.40 Nonetheless, in the personal data breach notification Fastway identified its staff training as a deficiency in the organisational measures that resulted in the personal data breach.[117] In fact, in this regard Fastway appears to propose to provide additional training to its own staff in order comply with its obligation to implement appropriate security and organisational measures on an ongoing basis.[118]

6.41 Regarding Data Protection Policies and Procedures, Fastway submitted that the Fastway Project Process[119] was used to map and realise IT projects. In particular, Fastway clarifies that:

> *"IT project management is a very controlled function within the Fastway / [IT Service Provider A] environment, and this is mapped and tracked using [redacted], and more recently, [redacted]. Tasks are divided into small steps and processed one after the other."*[120]

6.42 Whilst Fastway provided the DPC with its Fastway Project Process,[121] the DPC notes that the document provided is dated April 2021, two months after the personal data breach (23 February 2021). Therefore, the version submitted by Fastway is not indicative of an

[113] Fastway Submissions on the Draft Decision, dated 9 May 2022, page 9-10; 2018-05 email re New GDPR Regulations coming into effect; 2018-05 email re GDPR email notification; Parcel Connect website – GDPR changes.
[114] Fastway Submissions on the Commencement Letter and related attachments, dated 8 November 2021, page 6.
[115] Fastway Submissions on the Commencement Letter and related attachments, dated 8 November 2021, page 6.
[116] Fastway Submissions on the Commencement Letter and related attachments, dated 8 November 2021, page 6.
[117] In response to the query *"What deficiencies in these organisational or technical measures have been identified as a result of this breach?"* in the Personal Data Breach Notification, Fastway indicated: *"Security review by security lead and approval. Risk assessment process as part of security and data protection. Staff training as identified. Security Audits. Vulnerability compliance tools"*, cfr. Personal Data Breach Notification, dated 4 March 2021, page 3.
[118] Fastway indicated as actions to ensure compliance with security and organisational measures on an ongoing basis, among the various, *"Ensure additional training is undertaken and a log is updated/maintained"*, cfr., Fastway response to queries, dated 18 March 2021, page 18.
[119] D.7. Fastway Project Process.
[120] Fastway Submissions on the Commencement Letter and related attachments, dated 8 November 2021, page 8.
[121] D.7. Fastway Project Process.

appropriate standard of security at the time of the personal data breach. In its Submissions on the Draft Decision, Fastway underlined that the previous version was reviewed in February 2021, although it has not provided this version to the DPC.[122]

6.43 In its Submissions on the Draft Decision, Fastway also submitted the Fastway Change Management Policy, version dated 13 September 2019.[123] This procedure appears to be applicable to projects aimed at modifying aspects that have previously been fixed (*"Change Control is the process of handling proposed alterations to items that have been previously designated as fixed"*[124]), and it identifies a specific process, which included, for example, the phase related to *"investigate impact – configuration items to be changed, costs, timescales, risks"*[125] before the *"release"* of a change itself. Considering that the "Brexit project", as detailed above, consisted of a modification of the system, it seems that this Change Management Policy and procedure might have been applied to these circumstances. Nonetheless, as stated by Fastway and assessed above, Fastway did not perform a risk assessment before the decision to implement the "Brexit project".[126]

6.44 Fastway also provided its own Data Security Incident Management Procedure[127] to the DPC. This procedure was trigged by Fastway on 2 March 2021.[128] Following this procedure, Fastway not only identified the personal data breach and started the containment and recovery procedures, but also notified the personal data breach to the DPC and prepared the Incident Report.[129] This Data Breach Report was then furnished to Fastway's clients and the DPC.[130]

6.45 In the Personal Data Breach Notification[131] Fastway identified that, contrary to its own existing policies and procedures at the time of the personal data breach, the system changes were signed off verbally by a member of the Fastway IT and without the approval of the Data & Information Security representative. This was also further confirmed in the Fastway Data Breach Report:

> *"In this case, the approval was provided by* [redacted] *verbally to the developer, following a request which was raised with the IT team by Revenue to setup* [redacted] *in order to facilitate Brexit requirements.*

[122] Fastway Submissions on the Draft Decision, dated 9 May 2022, page 10.
[123] Fastway Submissions on the Draft Decision, dated 9 May 2022, page 10-11; Fastway Change Control Procedure.
[124] Fastway Change Control Procedure, page 1.
[125] Fastway Change Control Procedure, page 2.
[126] In the personal data breach notification, to the query on *"What deficiencies in these organisational or technical measures have been identified as a result of this breach"* Fastway reported: *"Security review by security lead and approval. Risk assessment process as part of security and data protection. Staff training as identified. Security Audits. Vulnerability compliance tools"*, cfr. Personal Data Breach Notification, dated 4 March 2021, page 3.
[127] Data Security Incident Management Procedure.
[128] Fastway response to queries, dated 18 March 2021, page 2.
[129] Data Security Incident Management Procedure.
[130] Data Breach Report.
[131] *"Irrespective of a system being considered internal, it should be subject to the same security controls as all our existing external facing applications. Failure to follow exiting process and security protocol perceived time constraints, and* ***instruction without approval from the appropriate person led to the breach***", (emphasis added), cfr. Personal Data Breach Notification, dated 4 March 2021, page 3.

Approval comes under the purview of the Data & Information Security representative, and in this case the approval was not obtained. This was a poor error in judgement placing the urgency of the task over the designated process. As this system was never intended to be made public, this resulted in substantial risk due to the request demanded by the [redacted]."[132]

6.46 In its Submissions on the Commencement Letter, Fastway further confirmed that:

> *"The* [redacted] *remained engaged throughout the process and had daily engagement with the Fastway team. Specifics were discussed and agreed to ensure proper rollout and in many instances verbal approval was provided to staff in order to progress with certain project actions with their team.*
> *[...]*
> *We have confirmed that* [redacted] *provided verbal approval for this aspect of the project, but we do have evidence that approval was provided* [redacted] *to [IT Service Provider A] via a skype conversation. You will see from the document attached that this relates directly to the actions contained within UAS20-155, copy of which is also included."*[133]

6.47 With reference to the evidence of the approval [redacted],[134] the DPC notes that this approval is dated 24 February 2021 at 7:58 pm. As the IT Security Report stated, Fastway's system was exposed from approximately 9am on 23 February 2021 to approximately 9am on 26 February 2021.[135] This was also confirmed by Fastway.[136]

6.48 In its Submissions on the Draft Decision, Fastway stated that the section on the initial personal data notification as reported above in para 6.45 *"was not accurate and arose due to the time pressures involved in submitting the necessary information to the DPC"*[137] and it submitted further documentation related to the ongoing dialogue between Fastway and the IT Service Provider A at the time of the personal data breach. Fastway appears also to consider that the evidence of the approval *"was in addition to the ongoing dialogue"*.[138] Fastway, then, concluded that it

> *"acknowledge[s] that the configuration was not checked to ensure that it was correct."*[139]

The further documentation provided by Fastway in its Submissions on the Draft Decision are twofold: some of the documents replicate what was previously provided by Fastway in

---

[132] Data Breach Report, page 6.
[133] Fastway Submissions on the Commencement Letter and related attachments, dated 8 November 2021, page 9.
[134] D.6. Approval via Skype.
[135] IT Security Report, page 9-10.
[136] Fastway response to queries, dated 18 March 2021, page 2.
[137] Fastway Submissions on the Draft Decision, dated 9 May 2022, page 11.
[138] Fastway Submissions on the Draft Decision, dated 9 May 2022, page 11.
[139] Fastway Submissions on the Draft Decision, dated 9 May 2022, page 11.

its Submissions on the Commencement Letter[140], and other documents refer to dialogue between Fastway and IT Service Provider A after the personal data breach happened.[141] In its Submissions on the Commencement Letter (as above reported), Fastway confirmed that the verbal approval was provided to the IT Service Provider A and this submission is not contended by Fastway in its Submissions on the Draft Decision.

6.49 Despite the ongoing dialogue as described by Fastway, I do not consider the verbal approval sufficient in circumstances where the technical features related to the system changes in the audience of the reporting system. Furthermore, this approval, although verbal, as identified in para 6.47, was given after the start of the personal data breach. Therefore, I consider that the approval provided by the [redacted] was not given appropriately in the context of the system changes since it was provided after the implementation of the system changes by IT Service Provider A and the start of the personal data breach. A proper approval should be provided before any action is undertaken.

6.50 Furthermore, whilst Fastway's [redacted] appears to have provided the verbal approval, I consider that the procedure for the approval of the "Brexit project" was not properly followed according to Fastway Data Protection Policies and Procedures in one crucial respect. As already assessed above in paragraphs 6.12, 6.13 and 6.35, the risk assessment was not performed as it should have been done before the implementation of the system changes in order to properly identify risks related to this change as well as any specific measures to mitigate the possible risks involving personal data.

6.51 In the Personal Data Breach Notification, Fastway specifically reported the following as measures taken in response to the personal data breach:

> *"Communicate to the entire team that no systems or application is exempt from the existing process"*[142].

As measures pending implementation at the time of the Personal Data Breach Notification (4 March 2021), Fastway further indicated:

> *"Review of approval process and ensure every member of the team including management are clear that no work can be deployed without sign off by appropriate person"*[143].

[140] In particular, Ticket UAS20-154 and Ticket UAS20-155 were provided in Fastway Submissions on the Commencement Letter, replicated also in its Submissions on the Draft Decision, dated 9 May 2022.
[141] In particular, Ticket UAS20-189, Ticket UAS20-199, Ticket UAS20-216 and Ticket UAS20-226 report exchange dialogue between Fastway and the IT Service Provider A from 26 February 2021 at 12:01 (after the personal data breach) to 17 March 2021 at 10:02. For avoidance of doubt, there is also another ticket UAS20-164, dated 15 February 2021, however it consists of only one message written by an employee on a specific work piece of work.
[142] Personal Data Breach Notification, dated 4 March 2021, page 3.
[143] Personal Data Breach Notification, dated 4 March 2021, page 4.

This was also later confirmed by Fastway.[144]

6.52 Finally, the DPC notes that Fastway appears to attribute some responsibility to IT Service Provider A (the development team) in terms of the way it conducted the implementation of the system changes causing consequently the personal data breach:

> *"Fastway are satisfied that **this breach resulted from an oversight within the development team**, and urgency of the request to fulfil Revenue requirements by the [redacted], causing the [redacted] application and associated [redacted] to be publicly accessible for the duration of the timeframe outlined above."*[145] (emphasis added)

Similarly, in its Submissions on the Draft Decision, Fastway remarked:

> *"Fastway relied on [IT Service Provider A] to execute this task properly and a configuration check was not conducted".*[146]

6.53 Its Submissions on the Draft Decision, Fastway also explained that it agreed a Statement of Work (the "**Statement of Work**") with the IT Service Provider A on 27 January 2021 for the "Brexit project",[147] detailing the service to be provided, the level of the experience of the development team and project management process to be followed.[148] In this regard, the DPC wishes to draw attention to section 12 of the Statement of Work, entitled "GDPR":

> *"[The IT Service Provider A] employees assigned to provide services under this contract usually do not access live data and they instead use test or sample data. Product Support personnel may sometimes get exposed to real-time data. in such events, [The IT Service Provider A] will take all reasonable efforts to assist in ensuring there is no data security breach. [The IT Service Provider A] agrees to follow any guidelines, checks and controls provided by Fastway in this regard."*[149]

6.54 As assessed in the above section on *IT Infrastructure and technical measures*, the personal data breach was indeed caused by a misconfiguration of the new system. However, it is my view that IT Service Provider A, as the developer team, was acting under the instructions of Fastway (more precisely the [redacted]). This appears also to be confirmed by the Statement of Work, as reported above, especially on data protection matters. In these circumstances Fastway (the [redacted]) appears to have disregarded the expected procedure of the approval. Fastway should have also overseen whether or not IT Service Provider A was technically implementing the system changes as required by the circumstances. It was Fastway's obligation pursuant to Article 32(1) of the GDPR to

[144] Fastway indicated among the actions to be taken to ensure compliance with security and organisational measures on an ongoing basis *"An immediate stop to all verbal instructions that concern any aspect that has the likely impact on data security."*, cfr. Fastway response to queries, dated 18 March 2021, page 18.
[145] Data Breach Report, page 9.
[146] Fastway Submissions on the Draft Decision, dated 9 May 2022, page 9.
[147] Fastway Submissions on the Draft Decision, dated 9 May 2022, page 2, point no 6.
[148] Fastway Submissions on the Draft Decision, dated 9 May 2022, page 2, point no 6.
[149] Statement of work, page 6.

properly instruct, check and oversee IT Service Provider A (the development team) such that personal data would be protected throughout the process.

6.55 It appears from the above description, therefore, that Fastway had some Data Protection Policies and Procedures in place. Nonetheless, at the time of requesting the system changes, Fastway did not follow these Data Protection Policies and Procedures on two crucial aspects: the staff did not request the approval of the Data & Information Security representative and instead signed off verbally themselves, in any case in disregard of the applicable procedure. Moreover, as previously analysed in detail, above all, the lack of the risk assessment negatively impacted Fastway's ability to identify and recognise the risks associated with this change. Therefore, I consider that the organisational measures implemented by Fastway were not appropriate since Fastway did not follow its own Data Protection Policies and Procedures, nor it appears where there were any "checks and balances" to ensure that these policies and procedures were fully followed by Fastway's staff.

6.56 In conclusion, due to the lack of risk assessment before the decision regarding the system changes, and the disregard of the expected procedure, I find that Fastway has failed to properly oversee IT Service Provider A (the developer team) and the implementation of the system changes.

iii. The Appropriate Level of Security

6.57 Fastway was obliged to implement appropriate technical and organisational measures to ensure a level of security appropriate to the low to moderate risk to the rights and freedoms of the data subjects. This required that, in the event of system changes, Fastway was obliged to implement technical and organisational measures to ensure that the appropriate level of security was maintained during and after the modifications. As detailed above, time constraints or perceived urgency (as also admitted by Fastway[150]) must not be considered a justification not to comply with Data Protection Regulations and internal Data Protection Policies and Procedures.

6.58 Article 32(1)(d) of the GDPR specifies that appropriate technical and organisational measures may include **regular** processes for testing, assessing and evaluating the effectiveness of existing measures. Such testing, assessing and evaluating applies to both **technical and organisational measures**. Personal data breaches may cause significant harm to data subjects and, pursuant to Article 32(1)(d), controllers and processors must take the initiative to test, assess, and evaluate their organisational and technical security measures regularly.

[150] Fastway identified, as another aspect related to the circumstances of the personal data breach, that *"Process review 2: urgency of the any task can never be allowed ignore following the process."*, cfr. Data Breach Report, page 9.

6.59 Fastway made submissions regarding its technical and organisational measures in the context of the personal data breach:

- *"Process review 1: the Information Security/Data Protection Staff should have been consulted when the* [redacted] *made a request that could allow data exposure.*
- *Process review 2: urgency of the any task can never be allowed ignore following the process.*
- *Process review 3: A Risk Assessment should have been conducted to carry out vulnerability identification, to review and address any changes or new risks in data protection by the way of security gap analysis.*
- *Process review 4: During the risk assessment, the* [redacted] *architectural issue and vulnerability could have been caught. All aspects should have been considered from data storage, remote access for other stakeholders and verify if the policies and procedures are adequate.*
- *Process review 5: our internal applications should all have the same security controls as our external facing applications which consist of vulnerability compliance management tools, threat monitoring tools, phishing tools etc. This would have allowed us to monitor security of data in motion as well as at rest and receive alerts when such incidents occur to prevent breach. This forms part of change control review and approval.*
- *Process review 6: Ensure that the staff handling data have adequate training on data security and information security approval workflows before handling any such requests."*[151]

6.60 With reference to the appropriateness of the technical and organisational measures implemented by Fastway at the time of the personal data breach, my views are the following.

6.61 An appropriate level of security required **technical measures** that have, *inter alia*, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services. The fact that the personal data stored [redacted] was not encrypted[152] and that Fastway system was never intended to be made public allowing access to external entities[153] contributed to the exploitation of the vulnerability introduced with the misconfiguration of the system. Therefore, I am of the view that the technical measures in place before the personal data breach were not appropriate to the low to moderate risk of Fastway's processing.

---

[151] Data Breach Report, page 9.

[152] Fastway response to further queries, dated 17 May 2021, page 2.

[153] In the Personal Data Breach Notification Fastway stated: *"Our internal reporting system are never publicly available – internal access procedures were only considered necessary in this respect, this was clearly a grave oversight. Irrespective of a system being considered internal, it should be subject to the same security controls as all our existing external facing applications. Failure to follow existing process and security protocols, perceived time constraints, and instruction without approval from the appropriate person lead to the breach"*, cfr. Personal Data Breach Notification, dated 4 March 2021, page 3. Furthermore, Fastway stated: *"At the time of our data breach the* [redacted] *table was not encrypted, this is what led to the exploitation of the vulnerability. This has been remedied since then."*cfr. Fastway response to further queries, dated 17 May 2021, page 2.

6.62 An appropriate level of security required **organisational measures** that enable Fastway to test, assess and evaluate the effectiveness of its security measures on a regular basis. In this regard, appropriate measures included conducting a risk assessment, especially in circumstances where technical or organisational changes are required and that may impact on processing operations concerning personal data. Fastway admitted that it did not perform a risk assessment before the decision to initiate the system changes and instructing IT Service Provider A.[154] Fastway acknowledged that, since its system (specifically [redacted] was never designed and intended to be made public, the system changes *"resulted in substantial risk due to the request demanded by the* [redacted] *"*[155]. The risk assessment would have enabled Fastway to be fully aware of the risks and to adopt the appropriate technical and organisational measures to prevent or (at least) mitigate the personal data breach.

6.63 Furthermore, appropriate measures also included the implementation of Data Protection Policies and Procedures appropriate to the risks presented by the processing operations, which must consider not only the appropriate training and awareness among the staff, but also include an oversight system to ensure that these internal Data Protection Policies and Procedures are correctly implemented and followed. These measures are particularly relevant when there is the intention to adopt a modification, which may have an impact or involve somehow processing of personal data, such as the system changes in an IT Infrastructure with servers storing personal data allowing access to an external entity. Fastway had in place such policies and procedures, however, as Fastway confirmed, its own staff did not follow them in the appropriate way in conducting the system changes.[156] I therefore consider these procedures were inadequate since they did not provide efficient oversight of compliance with the procedures themselves allowing Fastway to intervene in the erroneous authorisation process of the system changes. Secondly, in light of its data security obligations, Fastway should have properly overseen IT Service Provider A (the developer team) and the implementation of the system changes.

6.64 In its Submissions on the Draft Decision, Fastway acknowledged that if the data had been encrypted, it would not have been exposed.[157] However, Fastway disagreed on the appropriateness of the security measures in place at the time of the personal data breach, which it considered sufficient.[158] Furthermore, Fastway submitted that, despite the fact that a risk assessment was not conducted, the *"proper procedure [had] been followed in the course of this deliverable"*.[159]

---

[154] In the personal data breach notification, to the query on *"What deficiencies in these organisational or technical measures have been identified as a result of this breach"* Fastway reported: *"Security review by security lead and approval. Risk assessment process as part of security and data protection. Staff training as identified. Security Audits. Vulnerability compliance tools"*, cfr. Personal Data Breach Notification, dated 4 March 2021, page 3.

[155] Data Breach Report, page 6.

[156] Fastway reported as identified deficiencies of technical and organisational measures *"Failure to follow existing process and security protocols, perceived time constraints, and instruction without approval from the appropriate person lead to the breach"*, cfr. Personal Data Breach Notification, dated 4 March 2021, page 3.

[157] Fastway Submissions on the Draft Decision, dated 9 May 2022, page 11.

[158] Fastway Submissions on the Draft Decision, dated 9 May 2022, page 11.

[159] Fastway Submissions on the Draft Decision, dated 9 May 2022, page 11.

6.65 As detailed above in paras 6.62 and 6.63 (as well as in the previous Part 6.ii), in circumstances where Fastway decided to conduct a modification on the technical features of its system, aimed at modifying the audience for the reporting system, and despite that the risks were low to moderate, Fastway should have conducted the risk assessment to identify any possible risk arising from this specific change to the system before the start of the system change given its data security obligations, including but not limited to Article 32(1)(d) of the GDPR. Moreover, as explained above in paragraph 6.49, I do not consider that the approval within the procedure was sufficient, which was confirmed by Fastway to have been provided only verbally in its Submissions on the Commencement Letter[160] and in its Data Breach Report[161], prepared by Fastway for its clients. Nonetheless Fastway has not explained the reasons why the approval, although verbal via skype conversation, was provided the day after the start of the incident.

6.66 Accordingly, I find that Fastway infringed Article 32(1) of the GDPR by failing to implement a level of security appropriate to the risk. As outlined above, Fastway's failure to implement appropriate measures relates to both technical and organisational measures.

6.67 I note, however, that Fastway not only notified the personal data breach to the DPC, but also complied with part of its internal Data Protection Policies and Procedures, specifically the Data Security Incident Management Procedure, to contain the personal data breach, resolved the vulnerability and updated its own IT infrastructure to prevent similar incidents.

iv. Findings

6.68 In summary, therefore, it is my view that Fastway failed to implement the appropriate organisational and technical security measures to ensure an appropriate security level in relation to its processing of personal data for the provision of delivery services and stored in its internal report system [redacted] at the time of the personal data breach, and thereby infringed Article 32(1) of the GDPR.

---

[160] *"We have confirmed that the* [redacted] *provided verbal approval for this aspect of the project, but we do have evidence that approval was provided by* [redacted] *to [IT Service Provider A] via a skype conversation."*, cfr. Fastway Submissions on the Commencement Letter and related attachments, dated 8 November 2021, page 9.

[161] *"In this case, the approval was provided by* [redacted] *verbally to the developer, following a request which was raised with the IT team by Revenue to setup the DNS in order to facilitate Brexit requirements."*, cfr. Data Breach Report, page 6.

7. Corrective Powers

7.1 I have set out above, pursuant to section 111(1)(a) of the 2018 Act, my decision to the effect that Fastway has infringed Article 32(1) of the GDPR. Under section 111(2) of the 2018 Act, where the DPC makes a decision (in accordance with section 111(1)(a)), it must, in addition, make a decision as to whether a corrective power should be exercised in respect of the controller or processor concerned and, if so, the corrective power to be exercised. The remaining question for determination in this Decision is whether or not those infringements merit the exercise of any of the corrective powers set out in Article 58(2) and, if so, which one(s).

7.2 Recital 129 of the GDPR, which acts as an aid to the interpretation of Article 58, provides that *"... 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 ...."* In the circumstances of the within Decision, and with particular reference to the findings arising therefrom, I find that the exercise of one or more corrective powers is both appropriate, necessary and proportionate for the purpose of ensuring compliance with the GDPR.

7.3 Having carefully considered the infringement, I have decided to exercise corrective powers in accordance with section 115 of the 2018 Act and Article 58(2) of the GDPR. I set out below the corrective powers that are appropriate to address the infringement in the particular circumstances, and the reasons for that decision, having considered all of the corrective powers set out in Article 58(2). In summary, the corrective powers that I have decided to exercise are:

a) Article 58(2)(b) – I have decided to issue a reprimand to Fastway in respect of its infringement of Article 32(1) of the GDPR.
b) Article 58(2)(i) – I have decided to impose an administrative fine, pursuant to Article 83, in respect of Fastway's infringement of Article 32(1) of the GDPR.

A. Reprimand

7.4 I have decided to issue Fastway with a reprimand in respect of its infringement of Article 32(1) of the GDPR. Article 58(2)(b) provides that a supervisory authority shall have the power to *"issue reprimands to a controller or processor where processing operations have infringed provisions of this Regulation."* In accordance with Recital 129 of the GDPR, in imposing a corrective power, I must ensure that it is *"...appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case..."*.

7.5 I consider that a reprimand is appropriate, necessary and proportionate in view of ensuring compliance with the infringed Article as the reprimand, along with the other corrective measure, will act to formally recognise the serious nature of all of the infringement.

Further, the reprimand emphasises the requirement for Fastway to take all relevant steps to ensure continuous and future compliance with Article 32(1) of the GDPR.

7.6 Recital 148 of the GDPR is provides:

> *"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."*

7.7 Accordingly, it is clear from the GDPR that a reprimand does not have to be issued in isolation to the exercise of any other corrective power. In this respect, I consider it appropriate, necessary and proportionate to impose a reprimand in addition to the administrative fine in Part 7.B of this Decision. The decision to impose a reprimand is based on the serious nature of the infringement of Article 32(1) of the GDPR. The objective of this Article is to ensure that controllers and processors implement a level of security that is appropriate to the risk presented by their processing operations. Fastway's infringement of this Article is serious in light of the lack of appropriate technical and organisational measures. As detailed above in this Decision, Fastway had Data Protection Procedures and Policies in place, however, they were not followed at the time of the notified personal data breach. Having policies and procedures and not following them (and not designing checks and balances to verify the compliance with them) make them meaningless. This is particularly important when an organisation decides to adopt a modification to its own IT system that may involve or have an impact on the processing of personal data. Policies and procedures alone are not sufficient to mitigate risks to data subjects. Having considered that a controller or a processor must regularly assess and evaluate the effectiveness of measures in place and there must be an ongoing and verifiable oversight of how the staff members give effect to such policies and procedures. Pursuant to Article 32(1)(d) Fastway should have first conducted the risk assessment to identify and fully consider the risks for the rights and freedoms of natural persons related to the proposed system changes. The following events (such as the lack of encryption on the file containing personal data, the inappropriate verbal authorisation and the failure to oversee IT Service Provider A (the developer team), just to recall few of them, but all of them fully assessed in Part 6.ii and 6.iii above), again mainly based on the lack of compliance and lack of oversight of Fastway internal procedures, further contributed to circumstances leading to the notified personal data breach.

7.8 I consider that the imposition of a reprimand is both appropriate, necessary and proportionate in light of the importance of ensuring ongoing compliance with Article 32(1) of the GDPR in the context of protecting the fundamental rights and freedoms of data subjects. I consider that it is appropriate, necessary and proportionate to recognise the seriousness of non-compliance of this nature with a reprimand in light of that objective of ensuring compliance with Article 32(1) of the GDPR.

7.9 Therefore, I consider that the formal recognition of the seriousness of the infringement by means of a reprimand is appropriate and necessary to ensure compliance with this Article. A reprimand is proportionate in the circumstances where it does not exceed what is required to ensure compliance with the GDPR, taking into account the seriousness nature of the infringement and the potential for harm to data subjects.

B. Administrative Fine

7.10 In addition to the corrective power under Article 58(2)(b), I also consider that Fastway's infringement of Article 32(1) of the GDPR warrants the imposition of an administrative fine. The reason for that decision, and the method for calculating that fine, are set out below.

7.11 In its Submissions on the Draft Decision and in its Additional Submissions on the Draft Decision, Fastway submitted its request to waive or reduce the proposed administrative fine, addressing some of the criteria pursuant to Article 83(2) of the GDPR. I have considered those submissions, and I set out my consideration and analysis of Fastway's submissions with reference to the specific criteria pursuant to Article 83(2) of the GDPR below.

i. Whether the Infringement Warrant an Administrative Fine

7.12 Article 58(2)(i) permits the DPC to consider the imposition of an administrative fine, pursuant to Article 83, in addition to, or instead of, the other measures outlined in Article 58(2), depending on the circumstances of each individual case. This is also reflected in section 115 of the 2018 Act, which permits the DPC to impose an administrative fine on its own or in combination with any other corrective power specified in Article 58(2).

7.13 Article 83(1), in turn, identifies that the administration of fines *"shall in each individual case be effective, proportionate and dissuasive"*. In this context, when deciding whether or not to impose administrative fines and the amount of any such fines, I must give due regard to the criteria set out in Article 83(2) GDPR, which provide that:

> *"Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). 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:*
>
> *(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;*
>
> *(b) the intentional or negligent character of the infringement;*

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

(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;

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

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the categories of personal data affected by the infringement;

(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;

(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;

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

(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."

7.14 The decision as to whether to impose an administrative fine (and if so, the amount of the fine) is a cumulative decision which is taken having had regard to the factors as set out in Article 83(2)(a) to (k). Therefore, I will now proceed to consider each of these criteria in turn in respect of Fastway's infringement of Article 32(1) of the GDPR:

a) <u>the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;</u>

7.15 The nature of Fastway's infringement of Article 32(1) of the GDPR comprises a failure to comply with its obligation to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk in respect of its processing of personal data in respect of its provision of delivery services and its storage of personal data in its internal report system [redacted] at the time of the notified personal data breach. The objective of Article 32(1) is to protect the rights and freedoms of natural persons by ensuring that their personal data are processed in a manner that ensures appropriate security. This encompasses an ongoing obligation for testing, assessing and evaluating the effectiveness of existing measures in place to ensure such appropriate security. A failure

to implement an appropriate level of security increases the risk of personal data breaches. This, in turn, poses a threat to the rights and freedoms of data subjects because of the potential for damage to data subjects where personal data breaches occur. Therefore, compliance with Article 32(1) is central to the protection of the rights and freedoms of natural persons pursuant to the GDPR. As such, non-compliance with this obligation has serious consequences in that it has the potential to result in damage to data subjects.

7.16 I have also considered the gravity of the infringement of Article 32(1) of the GDPR and I have had regard to the nature, scope and purposes of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them. As detailed Part 6.i above, Fastway's processing at the time of the personal data breach involved low to moderate risks both in likelihood and severity to the rights and freedoms of data subjects. Although the significant quantity of personal data related to a large number of records, impacting 10,000 data subjects, processed and stored for a period of thirty (30) days by Fastway, this personal data may be considered at the lower end of the scale in terms of sensitivity.

7.17 In light of the above description of the gravity of the infringement having due regard of the nature, scope and purposes of the processing, objectively, I consider that the potential level of damage suffered by the data subjects was low to moderate. The failure to implement the appropriate technical and organisational measures led to the personal data breach. Therefore, I am of the view that Fastway's infringement of Article 32(1) of the GDPR is on the low to moderate of the scale of gravity.

7.18 Regarding the duration of the infringement of Article 32(1) of the GDPR, the personal data breach occurred on 23 February 2021. Fastway admitted that it did not perform a risk assessment before the decision to initiate the system changes and before instructing IT Service Provider A.[162] As detailed above in Part 6.ii and Part 6.iii, Fastway's technical and organisational measures in place before the system changes were not appropriate, which contributed to the notified personal breach.[163] In its Submissions on the Draft Decision, Fastway provided an overall description and related documentation on the systems and controls implemented to ensure data security prior to the personal data breach in 2020, as well as the Statement of Work signed between Fastway and the IT Service Provider A. In particular, this Statement of Work indicated that the Unified Analytics Systems (UAS)

[162] In the personal data breach notification, to the query on "*What deficiencies in these organisational or technical measures have been identified as a result of this breach*" Fastway reported: "*Security review by security lead and approval. Risk assessment process as part of security and data protection. Staff training as identified. Security Audits. Vulnerability compliance tools*", cfr. Personal Data Breach Notification, dated 4 March 2021, page 3.

[163] From a technical measures point of view, the personal data stored [redacted] was not encrypted (Fastway response to further queries, dated 17 May 2021, page 2); the security controls of its IT infrastructure were limited to internal access control procedures and these security controls were not the same as those existing in Fastway external facing applications (Personal Data Breach Notification, dated 4 March 2021, page 3). From an organisational measures point of view, internal Data Protection Policies and Procedures were not correctly implemented and followed (Personal Data Breach Notification, dated 4 March 2021, page 3) and Fastway did not properly oversee the implementation of the system changes conducted by IT Service Provider A.

project (the one originated the notified personal data breach)[164] was started on 1 January 2021.[165] Considering these recent submissions and the above reasoning as fully articulated in Part 6.ii and Part 6.iii, I consider the lack of the risk assessment before the implementation of the system change initiated a chain of events leading to the notified personal data breach. Therefore, I consider that the duration of the infringement must be assessed as commencing at 1 January 2021 and ending on the date of the personal data breach on 23 February 2021. Therefore, the duration is one month and 23 days in length. This Decision does not make findings in relation to the level of security that Fastway currently implements and it is acknowledged that Fastway implemented a number of additional measures following the discovery of the personal data breach.

b) <u>the intentional or negligent character of the infringement;</u>

7.19 The Article 29 Working Party Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679 ('the **Administrative Fines Guidelines**') provide that:

> *"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."*[166]

7.20 I do not consider that there was "*intent*" on the part of Fastway in respect of its infringement of Article 32(1) in the sense that there was "*knowledge*" or "*wilfulness*"" on the their part in respect of their failure to implement an appropriate level of security. However, I am satisfied that Fastway was negligent and breached the duty of care required of it by failing to implement the appropriate level of technical and organisational measures and oversee its Data Protection Policies and Procedures and IT Service Provider A.

7.21 In its Additional Submissions on the Draft Decision, Fastway underlined that there was no intent, however "*it seems extremely onerous on Fastway should the DPC form the ultimate view that there was negligence and/or breach of duty. Such a position may also have significant repercussions for Fastway, particularly in relation to any litigation claims that may be issued by data subjects pursuant to Article 82, GDPR*".[167] As clarified above, Article 32(1) of the GDPR obliges controllers and processors to implement a level of security appropriate to the risks presented by its processing of personal data and, in particular, Article 32(1)(d) of the GDPR requires regular processes for testing, assessing and evaluating the effectiveness of existing measures. Fastway not only failed to perform a risk assessment before the system changes, but, as detailed in Part 6.ii and Part 6.iii, it failed to

---

[164] Fastway Submissions on the Draft Decision, dated 9 May 2022, page 2, point no. 6.
[165] Statement of work, page 1.
[166] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679,* 17/EN, WP 253, adopted on 3 October 2017, endorsed by the EDPB on 25 May 2018, available at https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines_en (last) access on 11 March 2022, page 11.
[167] Fastway Additional Submission on the Draft Decision, dated 25 May 2022, page 2.

implement the appropriate level of technical and organisational measures. Therefore, in the circumstances, I consider that there was a negligent character to Fastway's infringement of Article 32(1) of the GDPR.

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

7.22 I find that Fastway took significant actions to mitigate the damage suffered by data subjects. Fastway became aware of the personal data breach on 24 February 2021 when an email was received by members of Fastway Franchise Support Office from an individual claiming to have gained access to an exposed server.[168] Fastway initially considered this to be a phishing email and forwarded it to IT Service Provider A for investigation on 25 February 2021.[169] On 26 February 2021 IT Service Provider A brought all access and permissions to the server under surveillance, and ended the vulnerability.[170] On 2 March 2021, after IT Service Provider A confirmed Fastway had been breached,[171] Fastway initiated the Incident Management Plan, which included investigating the event, timeline and adoption of various measures in response to the personal data breach.[172] It appears that Fastway completed the new configuration of its IT infrastructure on 8 March 2021 to replace the compromised one.[173] Therefore, I am satisfied that Fastway acted expeditiously in addressing the personal data breach and in implementing technical measures to re-establish the security of its systems.

7.23 On 5 March 2021 Fastway began contacting its clients with reference to the personal data breach and also completed the Data Breach Report on the same day.[174] Fastway stated that it notified 265,742 data subjects on behalf of its clients.[175] On 11 March 2021 Fastway also published a public statement on its website.[176] In its Submissions on the Draft Decision, Fastway confirmed that it has reviewed its internal protocols or implemented various measures to reduce the reoccurrence of such incident.[177] Fastway also added that it *"contracted an external company to conduct a deepweb search to identify if any data accessed during this incident had been leaked. The results came back in the negative."*[178] I consider that these actions helped to mitigate the damage suffered by data subjects affected by the personal data breach. This Decision does not make findings in relation to the level of security that Fastway currently implements and it is acknowledged that

[168] Fastway response to queries, dated 18 March 2021, page 1.
[169] Fastway response to queries, dated 18 March 2021, page 1.
[170] Fastway response to queries, dated 18 March 2021, page 1-2.
[171] Fastway response to queries, dated 18 March 2021, page 2.
[172] Personal Data Breach Notification, dated 4 March 2021, page 3-4.
[173] Fastway response to queries, dated 18 March 2021, page 4.
[174] Fastway response to queries, dated 18 March 2021, page 3.
[175] Fastway response to queries, dated 18 March 2021, page 9.
[176] Fastway response to queries, dated 18 March 2021, page 9.
[177] Fastway Submissions on the Draft Decision, dated 9 May 2022, page 9. For example, Fastway confirmed that it had extended technical security mechanisms to all external facing applications; it had also reviewed processes and controls including approvals, in order to ensure a separation of function between the development and testing environment.
[178] Fastway Submissions on the Draft Decision, dated 9 May 2022, page 6.

Fastway implemented a number of additional measures following the discovery of the personal data breach.

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;

7.24 As outlined above, Fastway infringed Article 32(1) of the GDPR by failing to implement appropriate technical and organisational measures regarding its processing in the context of the provision of delivery services and stored personal data in its internal report system [redacted] at the time of the personal data breach. I consider that Fastway holds a high degree of responsibility for this failure and that the absence of such measures must be deterred. However, in circumstances where this factor forms the basis for the finding of the infringement of Article 32(1) against Fastway, this factor cannot be considered aggravating in respect of this infringement.

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

7.25 There are no relevant previous infringements by Fastway.

f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

7.26 Fastway cooperated fully with the DPC to remedy the infringement and to mitigate its adverse effects. In its personal data breach notification (and updates), during the data breach handling process, as well as during the course of the Inquiry, it illustrated the steps that it had taken and was in the course of taking to remedy the infringement and the possible adverse effects. Part 6.ii details the steps, technical and organisational measures adopted and those proposed to be implemented by Fastway.

g) the categories of personal data affected by the infringement;

7.27 I consider that the categories of personal data affected by the infringement of Article 32(1) of the GDPR were at the lower end of the scale in terms of sensitivity. As outlined above, the personal data concerned names, home addresses, email addresses and mobile numbers. However, Fastway clarified that that these categories of personal data might not be fully present in each record, since the data collected depends on its clients and not all fields are mandatory.[179] Therefore, I consider that these categories of personal data do not represent an aggravating factor in the infringement of Article 32(1) of the GDPR.

[179] Fastway clarified *"In other words, the customer data provided by clients differs depending on the client. For example, some clients do not provide Fastway with customers' telephone numbers or email addresses. Therefore, the categories of data at A-E above is the full extent of personal data which was compromised in respect of each data subject and, in relation, to some data subjects, it would not have been all categories from A-E but a lesser subset."*, cfr., Fastway response to queries, dated 18 March 2021, page 8.

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;

7.28 Fastway's notification of the personal data breach indirectly contributed to the infringement becoming known to the DPC. The Administrative Fines Guidelines consider the relevance of such notifications regarding administrative fines:

> *"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."*[180]

7.29 As reported above in Part 2.ii, Fastway clarified in the course of the personal data breach handling process that in some cases it was a controller, in some a joint controller and in some other a processor.[181] In the specific circumstance of this case, Fastway's compliance with its own obligation as controller or joint controller to notify personal data breaches under Article 33(1) cannot be considered mitigating in respect of the infringement of Article 32(1) of the GDPR.

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;

7.30 The corrective powers have not previously been ordered against Fastway with regard to the subject-matter of this Draft Decision.

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

7.31 Not applicable.

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;

7.32 In its Submissions on the Draft Decision, Fastway also submitted additional elements for the DPC to consider in relation to the administrative fine. In particular, Fastway underlined that:

---

[180] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Guidelines on the application and setting of administrative fines, op. cit.*, page 15.

[181] Update Personal Data Breach Notification, dated 10 March 2021.

- it has spent *"significant time and expense"* to implement processes to ensure that incidents such as the notified personal data breach do not happen again[182];
- it has spent *"further expense"* related to the cost of the deepweb search by an external company;[183]
- it has *"incurred substantial legal costs"* related data subjects claims pursuant to Article 82 in terms of non-material damages claims;[184]
- it made various charity donations following the incident.[185]

7.33 I have considered the first two elements in the context of the assessment of the parameter pursuant to Article 83(2)(c) GDPR. With regard to the legal cost linked to non-material damages claims, it appears that Article 82 (Right to compensation and liability) and Article 83 (General conditions for imposing administrative fine) are aiming at two different and not cumulative purposes and functions: on one side, Article 82 is a direct action available to data subjects as a result of an infringement; on the other side, Article 83 is one of the corrective power available to supervisory authorities to ensure the application of the GDPR.[186] Lastly, the fact that Fastway made various charity donations cannot be taken into account as another mitigating factor pursuant Article 83(2)(k) of the GDPR to achieve a reduction of a proposal of the administrative fine. Considering such donations as a substitution or a sort of reduction/compensation from administrative fine may result in undermining the purpose of Article 83 of the GDPR, which is *"to strengthen the enforcement of the rules"* (as stated in Recital 148) and the intrinsic punitive and dissuasive nature of administrative fines as penalties. An administrative fine must be effective, proportionate and dissuasive in each individual case in accordance of Article 83. Thus, for the reasons as explained above, I do not consider the last two additional elements submitted by Fastway for the purpose of Article 83(2)(k) of the GDPR are mitigating.

---

[182] Fastway Submissions on the Draft Decision, dated 9 May 2022, page 14, point no. 2.
[183] Fastway Submissions on the Draft Decision, dated 9 May 2022, page 14, point no. 3.
[184] Fastway Submissions on the Draft Decision, dated 9 May 2022, page 15, point no. 4.
[185] Fastway Submissions on the Draft Decision, dated 9 May 2022, page 12, point no. 1.
[186] In this regard, please consider also the recent Advocate General Opinion on the case C-300/21 *UI v Österreichische Post AG*, where it is stated *"The GDPR repeats that model but strengthens the tools for ensuring the effectiveness of its provisions – which are now more detailed – and of the responses provided for – which are now more robust – in the event of an infringement or threat of infringement of those provisions: First, the GDPR broadens the role of supervisory authorities which, among other tasks, are responsible for imposing the harmonised penalties provided for therein. It thus emphasises the public enforcement component of the provisions. Second, it provides that individuals may take up the defence of the rights granted to them under the GDPR, either by triggering the procedure conducted by supervisory authorities (Article 77) or by bringing proceedings before the courts (Articles 79 and 82). In addition, Article 80 empowers certain bodies to bring representative actions, which makes the protection of general interests available to individuals easier."* (para 41), and *"As I have already pointed out, Article 82 of the GDPR forms part of a system of guarantees of the effectiveness of the rules in which private initiative supplements public enforcement of those rules. Compensation payable by data controllers or processors contributes to that effectiveness."* (para 45), and then *"Also in connection **with the separation of the functions of compensation and penalties**: When imposing a fine and setting its amount, the authority must take into account the factors set out in Article 83 of the GDPR, which are not provided for in the area of civil liability and which, in principle, may not be transferred to the calculation of damages. While the level of damage suffered by injured parties is a factor for adjustment of the fine, there is no reason why calculation of the amount of the fine should take account of any compensation the injured parties may have received."* (emphasis added), cfr. Case C-300/21 *UI v Österreichische Post AG*, Opinion of the Advocate General delivered on 6 October 2022 (ECLI:EU:C:2022:756).

7.34 Therefore, I consider that the matters considered under Article 83(2)(a) – (j) reflect an exhaustive account of both the aggravating and mitigating factors applicable in the circumstances of the case.

7.35 Given the specific circumstances of the case at hand, and having particular regard to the matters discussed under Article 83(2)(a) – (j) cumulatively, I consider it appropriate to impose an administrative fine in addition to the reprimand at Parts 7.A of this Decision.

7.36 When imposing corrective measure(s), I am obliged to select the measure(s) that are effective, proportionate and dissuasive in response to the particular infringements. The assessment of what is effective, proportionate and dissuasive must be made in the context of the objective pursued by the corrective measures. The Administrative Fines Guidelines provide that:

> *"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)."*[187]

7.37 I find that an administrative fine is necessary in order to effectively pursue the objective of re-establishing compliance by dissuading non-compliance with the Article 32(1) of the GDPR. Furthermore, I consider that an administrative fine is necessary in providing an effective, proportionate and dissuasive response in the particular circumstances of this case. In order to re-establish compliance with Article 32(1), it is necessary to dissuade non-compliance.

7.38 In reaching this decision to impose an administrative fine, I have had regard to all of the corrective powers available to me as set out in Article 58(2) of the GDPR. In particular, I have had regard to the reprimand in Part 7.A. The reprimand is of significant value in dissuading future non-compliance. This formal recognition of the seriousness of Fastway's infringement is likely to contribute to ensuring an appropriate level of security going forward.

7.39 However, having considered the nature of the infringement of Article 32(1), I consider that the reprimand alone is not effective and proportionate in dissuading future non-compliance. While I have had regard to the steps taken by Fastway to remedy the infringement, Article 32(1) places a continuous obligation on controllers and processors to regularly test, assess and evaluate the effectiveness of the technical and organisational measures that it has implemented. Furthermore, the appropriate level of security must be continually re-assessed in light of the dynamic risk presented by Fastway's processing and the state of the art.

---

[187] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Guidelines on the application and setting of administrative fines, op. cit.*, page 6.

7.40 In coming to the conclusion that an administrative fine is necessary and appropriate, I have particular regard to the nature, the gravity and the duration of the infringement (as assessed in accordance with Article 83(2)(a) above). This infringement posed a threat to the rights and freedoms of data subjects because of the potential for damage to data subjects where personal data breaches occur. I consider that an administrative fine is necessary in light of the potential for damage to data subjects by such non-compliance. This is because an administrative fine is necessary to effectively protect those rights by deterring future non-compliance.

7.41 Having found that the infringement identified warrants the imposition of an administrative fine in the circumstances of this case, I must next proceed to determine the amount of the administrative fine.

ii. The Applicable Range for the Administrative Fine

7.42 Having found that the infringement of Article 32(1) warrants the imposition of an administrative fine in the circumstances of this case, I must next proceed to determine the amount of that fine.

7.43 In the absence of specific EU-level guidelines on the calculation of fines in this context, I am not bound to apply any particular methodology[188]. In practical terms, this means that I am not bound to use a base figure or fixed financial starting point for the assessment of the proposed fine. Therefore, I ultimately intend to identify the amount of the administrative fine to be imposed on Fastway on a general basis (as in the judgments cited in the footnotes above) and by reference to the factors to which I am required to have due regard in accordance with Article 83(2) and which I have already applied to the circumstances of this case in detail above. In doing so, I must also ensure that, in accordance with the obligation on supervisory authorities under Article 83(1), the administrative fine imposed in this case is effective, proportionate and dissuasive.

7.44 In considering the application of the principles of effectiveness, proportionality and dissuasiveness of the administrative fine, I consider that a fine cannot be effective if it does not have significance relative to the revenue of the data controller or processor. Moreover, the principle of proportionality cannot be adhered to if the infringement is considered in the abstract, regardless of the impact on the controller or processor. This is compounded by the fact that future infringements need to be deterred. In this regard, I consider that a fine cannot be dissuasive if it will not be of any financial significance.

7.45 As regards the maximum amount for the fine that can be imposed, Article 83(4) of the GDPR provides that infringements of the obligations of controllers and processors pursuant to, amongst others, Article 32 shall:

---

[188] See by analogy Case T 332/09, *Electrabel v Commission,* judgement of 12 December 2012 (ECLI:EU:T:2012:672), para 228; Case T-704/14, *Marine Harvest ASA v Commission*, judgement of 26 October 2017 (ECLI:EU:T:2017:753), para 450.

"...in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher..."

7.46 The turnover of Fastway in 2020 was €53,994,415 as reported in Fastway's consolidated statement of comprehensive income for the 15 month financial period ended 31 March 2020 available from the Company Registration Office's public repository. As regards the maximum amount for the fine that may be imposed in this case, the relevant cap for any fine in respect of an infringement of Article 32(1) of the GDPR is up to €10,000,000 or up to 2% of the annual turnover of the preceding financial year, whichever is higher. Therefore, considering that the 2% of Fastway annual turnover in 2020 is €1,079,888.3, I am satisfied that the cap for Fastway's infringement is €10,000,000. This figure is not a starting point, but rather the cap on the permitted range as provided for in Article 83(4) of the GDPR.

7.47 The Draft Decision set out a proposed range for the administrative fine and the factors to be considered when calculating the fine in order to provide Fastway with the opportunity to comment in accordance with fair procedures. In its Submissions on the Draft Decision and in its Additional Submissions on the Draft Decision, Fastway submitted various comments on the administrative fines as outlined and assessed in above. Fastway also questioned whether the imposition of the administrative fine was necessary and submitted that, if the DPC would decide in favour of imposing a fine, the fine should be *"at the lower end of the range suggested by the DPC in its draft Decision"*.[189]

7.48 As set above, the permitted range for the infringement of Article 32(1) of the GDPR is up to €10,000,000 as provided for in Article 83(4) of the GDPR. In locating the administrative fine on the permitted range, I have had particular regard to the nature, the gravity and the duration of the infringement as assessed in accordance with Article 83(2)(a) above. I have also had regard to the aggravating factor, specifically the negligent character of the infringement as assessed in accordance with Article 83(2)(b) above. I have also had regard to the mitigating factors. Specifically, I consider as mitigating the actions taken by Fastway to mitigate the damage suffered by data subjects as identified above under Articles 83(2)(c), the absence of any relevant previous infringements as identified above under Articles 83(2)(e), and the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement as identified above under Article 83(2)(f) of the GDPR. Therefore, having regard to all of these factors, I consider that the administrative fine of **€15,000** is appropriate in the circumstances of this case.

7.49 I consider that the above administrative fine meets the requirements of effectiveness, proportionality and dissuasiveness. In order for any fine to be effective, it must reflect the circumstances of the individual case. The circumstances of this infringement concerns Fastway's failure to implement appropriate technical and organisational measures to

[189] Fastway Additional Submission on the Draft Decision, dated 25 May 2022, page 2.

ensure the appropriate level of security to the risk of the processing of personal data in respect of its provision of delivery services and its storage of personal data in its internal report system [redacted]. This failure led ultimately to a personal data breach, involving a significant number of data subjects, exposing them to potential damage, such as loss of control over their personal information, identify theft or fraud, or nuisance calls. I consider that these circumstances require a significant fine in order for it to be effective. In order for a fine to be dissuasive, it must dissuade the controller from repeating the conduct concerned. I am satisfied that the administrative fine would be dissuasive to Fastway. As regards the requirement for any fine to be proportionate, this requires me to adjust the quantum of any proposed fine to the minimum amount necessary to achieve the objectives pursued by the GDPR. I am satisfied that the administrative fine identified above does not exceed what is necessary to enforce compliance with the GDPR. Accordingly, I am satisfied that the administrative fine identified above would be effective, proportionate and dissuasive, taking into account all of the circumstances of this case.

8. Right of Appeal

8.1 This Decision is issued in accordance with section 111 of the 2018 Act. Pursuant to section 150(5) of the 2018 Act, Fastway has the right to appeal against this Decision within 28 days from the date on which notice of the Decision is received by it. Furthermore, pursuant to section 142 of the 2018 Act, as this Decision includes a decision to impose an administrative fine, Fastway has also have the right to appeal against that decision within 28 days from the date on which notice of this Decision is given to it.