Data Protection Act 2018

2018 CHAPTER 12

PART 6

ENFORCEMENT

Penalties

155 Penalty notices

(1) If the Commissioner is satisfied that a person—

(a) has failed or is failing as described in section 149(2), (3), (4) or (5), or

(b) has failed to comply with an information notice, an assessment notice or an enforcement notice,

the Commissioner may, by written notice (a "penalty notice"), require the person to pay to the Commissioner an amount in sterling specified in the notice.

(2) Subject to subsection (4), when deciding whether to give a penalty notice to a person and determining the amount of the penalty, the Commissioner must have regard to the following, so far as relevant—

(a) to the extent that the notice concerns a matter to which the GDPR applies, the matters listed in Article 83(1) and (2) of the GDPR;

(b) to the extent that the notice concerns another matter, the matters listed in subsection (3).

(3) Those matters are—

(a) the nature, gravity and duration of the failure;

(b) the intentional or negligent character of the failure;

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

(d) the degree of responsibility of the controller or processor, taking into account technical and organisational measures implemented by the controller or processor in accordance with section 57, 66, 103 or 107;

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

(f) the degree of co-operation with the Commissioner, in order to remedy the failure and mitigate the possible adverse effects of the failure;

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

(h) the manner in which the infringement became known to the Commissioner, including whether, and if so to what extent, the controller or processor notified the Commissioner of the failure;

(i) the extent to which the controller or processor has complied with previous enforcement notices or penalty notices;

(j) adherence to approved codes of conduct or certification mechanisms;

(k) any other aggravating or mitigating factor applicable to the case, including financial benefits gained, or losses avoided, as a result of the failure (whether directly or indirectly);

(l) whether the penalty would be effective, proportionate and dissuasive.

(4) Subsections (2) and (3) do not apply in the case of a decision or determination relating to a failure described in section 149(5).

(5) Schedule 16 makes further provision about penalty notices, including provision requiring the Commissioner to give a notice of intent to impose a penalty and provision about payment, variation, cancellation and enforcement.

(6) The Secretary of State may by regulations—

(a) confer power on the Commissioner to give a penalty notice in respect of other failures to comply with the data protection legislation, and

(b) provide for the maximum penalty that may be imposed in relation to such failures to be either the standard maximum amount or the higher maximum amount.

(7) Regulations under this section—

(a) may make provision about the giving of penalty notices in respect of the failure,

(b) may amend this section and sections 156 to 158, and

(c) are subject to the affirmative resolution procedure.

(8) In this section, "higher maximum amount" and "standard maximum amount" have the same meaning as in section 157.

156 Penalty notices: restrictions

(1) The Commissioner may not give a controller or processor a penalty notice in reliance on section 149(2) with respect to the processing of personal data for the special purposes unless—

(a) a determination under section 174 with respect to the data or the processing has taken effect, and

(b) a court has granted leave for the notice to be given.

(2) A court must not grant leave for the purposes of subsection (1)(b) unless it is satisfied that—

(a) the Commissioner has reason to suspect a failure described in section 149(2) which is of substantial public importance, and

(b) the controller or processor has been given notice of the application for leave in accordance with rules of court or the case is urgent.

(3) The Commissioner may not give a controller or processor a penalty notice with respect to the processing of personal data where the purposes and manner of the processing are determined by or on behalf of either House of Parliament.

(4) The Commissioner may not give a penalty notice to—

(a) the Crown Estate Commissioners, or

(b) a person who is a controller by virtue of section 209(4) (controller for the Royal Household etc).

(5) In the case of a joint controller in respect of the processing of personal data to which Part 3 or 4 applies whose responsibilities for compliance with that Part are determined in an arrangement under section 58 or 104, the Commissioner may only give the controller a penalty notice in reliance on section 149(2) if the controller is responsible for compliance with the provision, requirement or principle in question.

157 Maximum amount of penalty

(1) In relation to an infringement of a provision of the GDPR, the maximum amount of the penalty that may be imposed by a penalty notice is—

(a) the amount specified in Article 83 of the GDPR, or

(b) if an amount is not specified there, the standard maximum amount.

(2) In relation to an infringement of a provision of Part 3 of this Act, the maximum amount of the penalty that may be imposed by a penalty notice is—

(a) in relation to a failure to comply with section 35, 36, 37, 38(1), 39(1), 40, 44, 45, 46, 47, 48, 49, 52, 53, 73, 74, 75, 76, 77 or 78, the higher maximum amount, and

(b) otherwise, the standard maximum amount.

(3) In relation to an infringement of a provision of Part 4 of this Act, the maximum amount of the penalty that may be imposed by a penalty notice is—

(a) in relation to a failure to comply with section 86, 87, 88, 89, 90, 91, 93, 94, 100 or 109, the higher maximum amount, and

(b) otherwise, the standard maximum amount.

(4) In relation to a failure to comply with an information notice, an assessment notice or an enforcement notice, the maximum amount of the penalty that may be imposed by a penalty notice is the higher maximum amount.

(5) The "higher maximum amount" is—

(a) in the case of an undertaking, 20 million Euros or 4% of the undertaking's total annual worldwide turnover in the preceding financial year, whichever is higher, or

(b) in any other case, 20 million Euros.

(6) The "standard maximum amount" is—

(a) in the case of an undertaking, 10 million Euros or 2% of the undertaking's total annual worldwide turnover in the preceding financial year, whichever is higher, or

(b) in any other case, 10 million Euros.

(7) The maximum amount of a penalty in sterling must be determined by applying the spot rate of exchange set by the Bank of England on the day on which the penalty notice is given.

158 Fixed penalties for non-compliance with charges regulations

(1) The Commissioner must produce and publish a document specifying the amount of the penalty for a failure to comply with regulations made under section 137.

(2) The Commissioner may specify different amounts for different types of failure.

(3) The maximum amount that may be specified is 150% of the highest charge payable by a controller in respect of a financial year in accordance with the regulations, disregarding any discount available under the regulations.

(4) The Commissioner—

(a) may alter or replace the document, and

(b) must publish any altered or replacement document.

(5) Before publishing a document under this section (including any altered or replacement document), the Commissioner must consult—

(a) the Secretary of State, and

(b) such other persons as the Commissioner considers appropriate.

(6) The Commissioner must arrange for a document published under this section (including any altered or replacement document) to be laid before Parliament.

159 Amount of penalties: supplementary

(1) For the purposes of Article 83 of the GDPR and section 157, the Secretary of State may by regulations—

(a) provide that a person of a description specified in the regulations is or is not an undertaking, and

(b) make provision about how an undertaking's turnover is to be determined.

(2) For the purposes of Article 83 of the GDPR, section 157 and section 158, the Secretary of State may by regulations provide that a period is or is not a financial year.

(3) Regulations under this section are subject to the affirmative resolution procedure.