EXPLANATORY MEMORANDUM TO

THE PRIVACY AND ELECTRONIC COMMUNICATIONS (EC DIRECTIVE) (AMENDMENT) REGULATIONS 2015

2015 No. 355

1. This explanatory memorandum has been prepared by the Department for Culture Media and Sport and is laid before Parliament by Command of Her Majesty.

2. Purpose of the instrument

2.1 This Instrument amends the Privacy and Electronic Communications Regulations 2003 ("the 2003 Regulations") which regulate privacy and data protection in the electronic communications sector in the UK. The amendments do two things: firstly they permit Mobile Network Operators to send alert messages to those who may be affected by a serious emergency when requested to do so by a designated public body; and secondly they lower the legal threshold at which the Information Commissioner's Office ("ICO") can issue a civil monetary penalty ("CMP") for a serious breach of regulations 19 to 24 of the 2003 Regulations concerning unsolicited calls, texts, fax messages and electronic mail.

3. Matters of special interest to the Joint Committee on Statutory Instruments

3.1 None

4. Legislative Context

4.1 The making of this instrument is subject to the negative resolution procedure. A Transposition Note has been produced and is attached to this Memorandum.

4.2 The 2003 Regulations were made to implement the provisions of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector ("the Directive") in the UK. They were made using the power in section 2(2) of the European Communities Act 1972 ("the Act"). The Directive is one of a family of five Directives which formed the original European Electronic Communications Framework and were implemented within the UK by means of the Communications Act 2003, the Wireless Telegraphy Act 2006 and the 2003 Regulations.

4.3 The 2003 Regulations were amended in 2004 (S.I. 2004/1039) to permit corporate subscribers to register their telephone number with the Telephone Preference Service

("TPS") and in 2010 to replace the relevant tribunals under regulation 28 with the newly created first-tier tribunal and upper tribunal. The 2003 Regulations were amended for a third time in 2011 (S.I. 2011/1208) ("the 2011 Amendments") to implement further European legislative changes, namely Articles 2 and 3 of Directive 2009/136/EC, which in turn amended Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and service, Regulation (EC) No 2006/2004 on co-operation between national authorities responsible for the enforcement of consumer protection law and the Directive.

Emergency alerts

4.4 Regulations 7 and 8 of the 2003 Regulations restrict the purposes for which traffic data[1] can be processed and how the data can be retained. Regulation 14 places limitations on the processing of location data[2] without the consent of the user or subscriber. The restrictions in regulations 7(1), 8(2), 14(2) and 14(5) would prevent mobile network operators from operating an emergency alert service.

4.5 Articles 1(3) and 15(1) of the Directive enable its provisions regarding the processing of traffic and location data to be restricted in relation to activities concerning public security, defence and state security. The provisions of this instrument that relate to the emergency alert service concern the safeguarding of public security. They permit mobile network operators (defined as "relevant public communications providers")[3], in emergency situations, to disregard certain restrictions on processing data for the purposes of sending alert messages on behalf of the authorities. Activities concerning state security are already exempt under the 2003 Regulations by virtue of regulation 28.

ICO threshold

4.6 Regulations 19 to 24 of the 2003 Regulations provide rules that organisations must comply with, when sending marketing and advertising by electronic means (e.g. phone or text) or by using an automated calling system.

[1] Traffic data is defined by the 2003 Regulations as "any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing in respect of that communication and includes data relating to the routing, duration or time of a communication."

[2] Location data is defined by the 2003 Regulations as "any data processed in an electronic communications network indicating the geographical position of the terminal equipment of a user of a public electronic communications service, including data relating to—

a. the latitude, longitude or altitude of the terminal equipment;
b. the direction of travel of the user; or
c. the time the location information was recorded.

[3] A "relevant public communications provider" is a person who-

a. provides a public electronic communications network;
b. provides cellular mobile electronic communications services; and
c. holds a wireless telegraphy licence granted under section 8 of the Wireless Telegraphy Act 2006.

4.7 The 2011 Amendments amended regulation 31 of the 2003 Regulations to extend sections 55A to 55E of the Data Protection Act 1998 ("the DPA 1998") (which were inserted into the DPA 1998 by section 144(1) of the Criminal Justice and Immigration Act 2008). Those provisions of the DPA 1998 have effect under the 2003 Regulations subject to the modifications set out in Schedule 1 of the 2003 Regulations. The importation of the modified section 55A of the DPA 1998 provides a power to the Information Commissioner to impose a CMP providing certain conditions are met. That CMP may be a sum up to a maximum of £500,000 (see the Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010 (S.I. 2010/31)).

4.8 The required conditions to impose a CMP, as introduced by the 2011 Amendments, were that the Information Commissioner is satisfied that: there has been a serious contravention of the requirements of the 2003 Regulations; the contravention was of a kind likely to cause substantial damage or substantial distress, and the contravention was deliberate or the person knew or ought to have known that there was a risk of such a contravention and failed to take reasonable steps to prevent it.

4.9 The ICO issued guidance, under section 55C of the DPA 1998, about the issuing of CMPs under the 2003 Regulations, as amended in 2011. That guidance, amongst other matters, addressed the term 'substantial' in relation to damage and distress stating that the Commissioner considers that '…if damage or distress that is less than considerable in each individual case is suffered by a large number of individuals the totality of the damage or distress can nevertheless be substantial'. In October 2013 however, the First-tier (Information Rights) Tribunal did not support this approach and overturned the Commissioner's decision to issue a CMP in that case (EA/2012/0260). The First-tier Tribunal's Decision was subsequently upheld by the Upper Tribunal ([2014] UKUT 0255 (AAC)).

4.10 These Regulations amend Schedule 1 of the 2003 Regulations to adopt a lower threshold at which the Information Commissioner can issue a CMP on companies or persons who have contravened Regulations 19, 20, 21, 22, 23 or 24 of the 2003 Regulations. The test for imposition of a CMP for contravention of those regulations, as set out in paragraph 8AA of the Schedule, removes the condition that the contravention must have been "of a kind likely to cause substantial damage or substantial distress".

4.11 In lowering the threshold, and in response to the Tribunals' decisions, the UK is seeking to ensure that the penalty regime is 'effective, proportionate and dissuasive' as required by Article 15a of the Directive, as amended by Directive 2009/136/EC.

5. Territorial Extent and Application

5.1 This instrument applies to all of the United Kingdom.

6. European Convention on Human Rights

6.1 The Minister of State for Culture and the Digital Economy, Ed Vaizey, has made the following statement regarding Human Rights:

In my view the provisions of the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2015 are compatible with Convention rights.

7. Policy background

7.1 This explanatory memorandum has been produced in collaboration with the Cabinet Office, the Department leading the policy on emergency alerts.

Emergency alerts

7.2 The 2010 Strategic Defence and Security Review committed the Government to evaluating options for an improved Public Emergency Alert system. The Cabinet Office has been working to fulfil this and based on research and societal trends has considered an approach that would be capable of sending messages to mobile devices. This would provide a limited number of authorities, including the police, with the capability to send messages to mobile devices believed to be in the area of an emergency. The message would provide important advice to the recipient of specific action they should take to limit the emergency's impact on them. The system could also be available for use by those organisations across the UK who are responsible for issuing official flood warnings.

7.3 A series of live trials held in 2013 concluded that a Location-Based SMS approach would be the best way forward[4]. These trials were completed in partnership with local emergency responders and the three largest mobile network operators. Public focus groups were held and findings analysed by experts from the Behavioural Sciences team at Public Health England. Following the trials, further work with the mobile network operators looked at the practicalities of implementing such a system. This identified that the current 2003 Regulations would prevent the processing of data essential to identify devices thought to be in affected areas unless it was a consent-based system.

7.4 The scenarios where alert messages might be employed are likely to fall within the meaning of an emergency in the Civil Contingencies Act 2004. This includes severe flood

[4] Final Report into the Mobile Alert Trials, Cabinet Office, March 2014; https://www.gov.uk/government/publications/mobile-alerting-trials-for-public-emergencies

events, serious chemical accidents or very large fires. A periodic testing programme will be necessary to ensure the system remains operational and available for use.

7.5 This amendment permits certain communications providers to disregard a number of restrictions on the processing data set out in regulations 7, 8 and 14 for the purposes of issuing an emergency alert message or testing the system, provided a request to do so has been received from an organisation or person listed in these Regulations.

7.6 It also permits network operators to store traffic and location data processed for the purposes of sending an emergency alert for up to 7 days (48 hours in the case of testing), at which point the data must be erased or anonymised. This will allow all devices that have previously received an alert during an incident to be sent important updates, including 'all clear' messages to those who have been evacuated from an area.

7.7 In order to be an effective means of warning and informing the public in an emergency, the system must be capable of being activated 24 hours a day, 7 days a week. Work with emergency responders and the Association of Chief Police Officers (ACPO) has concluded that, in most scenarios, the Police are likely to be best placed to issue alert messages. Other bodies might, however, take the lead in certain circumstances, for example, environmental agencies in relation to severe flooding.

7.8 Given the likely impact of the scenarios where alert messages will be sent, the provisions to temporarily permit the major mobile network operators to process traffic and location data for this purpose are proportionate. Constraining this to the most serious emergencies where the mobile networks are requested to do so by a limited number of public authorities and in accordance with their directions serves to maintain control over the use of the alert system.

ICO threshold

7.9 The Government committed to consulting on lowering the legal threshold for ICO in its Nuisance Calls Action Plan that was published on 30 March 2014.

7.10 Under the 2003 Regulations, unsolicited marketing calls should not be made to anyone who has registered their number with the TPS, or who has previously advised the caller not to make further calls to them. Similarly consumers must not receive unsolicited SMS text messages unless they have either given prior consent or there is an existing relationship with the organisation being marketed. The 2003 Regulations implement a series of European provisions which include that the penalty regime for breaching the regulations must be effective proportionate and dissuasive.

7.11 The ICO is responsible for enforcing the 2003 Regulations. There are a variety of actions that can be taken to do so, including issuing notices for information, serving enforcement notices and conducting a compulsory audit of compliance. In addition, and of relevance to these Regulations, the Commissioner has power, via the 2003 Regulations' extension of the DPA 1998 to issue a CMP of up to £500,000 for breaches of the 2003 Regulations. Prior to this instrument, in order to issue a CMP, the ICO had to be satisfied that there was a serious breach of the 2003 Regulations; that it was of a kind that was likely to cause substantial damage or substantial distress and that the contravention was deliberate or the person knew or ought to have known that there was a risk of such a contravention and failed to take reasonable steps to prevent it.

7.12 Whilst there has been some success in bringing enforcement action under that regime, the issue of nuisance and spam communications continues to be a major concern for consumers and complaint volumes have increased substantially in recent years with 84% of consumers who participated in a study by Ofcom last year reporting that they received at least one nuisance call on their landline in a four week period[5]. The issue has also been the subject of a Which? campaign, attracting over 141,985 signatures as well as a number of parliamentary debates.

7.13 CMPs have played a key role in reducing the volume of non-compliant behaviour. In November 2012, following the issue of a monetary penalty to two individuals (later overturned on appeal), Cloudmark, who run the GSMA's 7726 spam text short code reporting service, identified a significant reduction (10% of all spam SMS) being sent that month compared to the previous month. Since January 2012, the ICO has been able to issue nine CMPs totalling £815,000 but some organisations that have deliberately made a large number of unsolicited direct marketing calls or sent numerous unsolicited SMS text messages have not been issued with CMPs because the ICO is unable to prove the conditions in the modified section 55A DPA 1998 are met.

7.14 Additionally, the First-tier (Information Rights) Tribunal (upheld on appeal to the Upper Tribunal) overturned a CMP issued by the ICO in one instance on the basis of a lack of evidence that such practice caused substantial damage or substantial distress, demonstrating that the ICO's ability to regulate this practice effectively is curtailed by the legal threshold required by the 2011 Amendments. It is estimated that if a lower threshold had been in place for the period 1 April 2012 to 31 November 2012, then approximately 50 additional organisations could have been considered for enforcement action which

[5] Landline Nuisance Calls Panel Wave 2 report 2014, published 23 Mary 2014 at http://stakeholders.ofcom.org.uk/market-data-research/other/telecoms-research/nuisance_calls_research/ - last accessed 12 February 2015

would include 'repeat offenders' who feature in the ICO's list of persistent offenders every month.

7.15 A lower legal threshold will allow the ICO to issue a wider range of smaller penalties, as well as being able to continue concentrating on larger cases. It is expected that this combined approach, will have a more powerful effect on organisations that are breaking the law by making and sending unsolicited communications.

8. Consultation outcome

Emergency alerts

8.1 The Government consulted on its proposals to make these amendments. A six-week consultation was launched in December 2014 outlining the Government's preferred approach. A total of 27 responses were received. Given the UK-wide extent of these regulations the Devolved Administrations were consulted as was the ICO who is responsible for enforcing the 2003 Regulations.

8.2 The consultation found that there was broad support for the proposal to make targeted and specific amendments to the 2003 Regulations to enable the future operation of an alert system. Many of the responses commented that any future system should only be used in the event of a serious emergency, and as such trigger points for use would need to be at a sufficiently high threshold, robust security arrangements would need to be in place around the system and any future implementation would require a thorough and detailed accompanying communications strategy. Discussions with a number of civil society organisations which have an interest in the area of data privacy also informed the response to the consultation.

8.3 A full analysis of the consultation report is available online at: https://www.gov.uk/government/consultations/changing-existing-regulations-for-an-emergency-alert-system.

ICO threshold

8.4 A consultation was launched on 25 October 2014 and closed on 6 December 2014. A total of 298 responses were received.

8.5 The consultation presented three options for reform: 1) Do nothing 2) Lower the legal threshold to 'annoyance, inconvenience or anxiety' 3) Remove the existing legal threshold of 'substantial damage or substantial distress'.

8.6 The majority of respondents, who expressed a preferred option, chose option 3 and there was broad support for the Government to take action against nuisance calls from other respondents.

8.7 The Government response to the consultation is available online at: https://www.gov.uk/government/consultations/nuisance-calls-consultation.

9. Guidance

Emergency alerts

9.1 No further guidance will be issued for the amendment on emergency alerts. However, work will continue with mobile network operators to put a framework for implementing an alert service in place. It is envisaged a protocol for authorities on using the emergency alert system will be developed and the current intention is to consult on this.

ICO threshold

9.2 ICO publishes guidance[6] on the 2003 Regulations for organisations who wish to send electronic marketing messages. This will be updated to reflect this amendment.

10. Impact

Emergency alerts

10.1 A regulatory impact assessment has been prepared in respect of regulation 2(2) of this instrument and is attached to this Memorandum. The impact on the telecommunications sector is minimal. This amendment is permissive – it would enable (rather than mandate) mobile network operators to send emergency alert messages. The direct cost of this regulatory change would be a transitional familiarisation one and this is estimated at £5,000 per mobile communications company and £3,500 per fixed communication provider. Apart from this, no direct costs are imposed as this is a permissive regulation and it will be optional for communications companies. The cost of operating an alert system is excluded from this assessment and will be the subject of further discussions with the network operators in question.

10.2 The direct costs to the public sector of this change are negligible. There would however be cost involved in implementing any new alert system. This would include technology development, rolling this out for use and ongoing running costs.

ICO threshold

10.3 The impact on business, charities or voluntary bodies is zero net cost for any compliant business. The proposal will only impact on non-compliant businesses that are in breach of the legal requirements of regulations 19 to 24 of the 2003 Regulations. These non-compliant businesses will be more likely to be subject to CMPs and less likely to be

[6] https://ico.org.uk/for-organisations/guide-to-pecr/ - last accessed 11 February 2015

able to overturn them on appeal giving them a more effective incentive to become compliant.

10.4 Effective punishment of non-compliant businesses will also bring benefits to those that are compliant as they will no longer have to compete with those gaining an advantage by acting illegally but not being punished. There may also be some benefits for companies who are incentivised to become compliant, in terms of lower levels of complaints and therefore lower costs in dealing with those complaints.

10.5 The known and direct costs to the public sector are negligible. At the time of the Government response to consultation, the ICO advised that they have resources in place to handle the anticipated increase in workload.

10.6 An Impact Assessment has therefore not been prepared for regulations 2(3) to 2(5) of this instrument.

11. Regulating small business

Emergency alerts

11.1 The amendment to the 2003 Regulations regarding mobile alerts apply equally to all main mobile network operators, which are large organisations.

ICO threshold

11.2 The 2003 Regulations concerning the ICO threshold, as amended, will continue to apply to small businesses, as it has done to date. Only non-compliant businesses will be impacted by the amendment.

12. Monitoring & review

Emergency alerts

12.1 The Cabinet Office, working with the Information Commissioner will review the parts of the amendment concerning emergency alerts 24 months after the changes come in to force.

ICO threshold

12.2 The Department for Culture, Media and Sport will continue to monitor the level of nuisance calls, working with the Information Commissioner and the Office of Communications.

13. Contact

David Barnes at the Cabinet Office, tel 020 7276 5401: email david.barnes@cabinet-office.x.gsi.gov.uk can answer any queries relating to emergency alerts in the Instrument.

Ihtsham Hussain at the Department for Culture Media and Sport tel: 020 7211 6140 or email: ihtsham.hussain@culture.gov.uk can answer any queries relating to the ICO threshold in the instrument.