
STATUTORY INSTRUMENTS

2002 No. 318

The Electronic Signatures Regulations 2002

Citation and commencement

1. These Regulations may be cited as the Electronic Signatures Regulations 2002 and shall come into force on 8th March 2002.

Interpretation

2. In these Regulations—

“advanced electronic signature” means an electronic signature—

- (a) which is uniquely linked to the signatory,
- (b) which is capable of identifying the signatory,
- (c) which is created using means that the signatory can maintain under his sole control, and
- (d) which is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

“certificate” means an electronic attestation which links signature-verification data to a person and confirms the identity of that person;

“certification-service-provider” means a person who issues certificates or provides other services related to electronic signatures;

“Directive” means Directive [1999/93/EC](#) of the European Parliament and of the Council on a Community framework for electronic signatures⁽¹⁾;

“electronic signature” means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication;

“qualified certificate” means a certificate which meets the requirements in Schedule 1 and is provided by a certification-service-provider who fulfils the requirements in Schedule 2;

“signatory” means a person who holds a signature-creation device and acts either on his own behalf or on behalf of the person he represents;

“signature-creation data” means unique data (including, but not limited to, codes or private cryptographic keys) which are used by the signatory to create an electronic signature;

“signature-creation device” means configured software or hardware used to implement the signature-creation data;

“signature-verification data” means data (including, but not limited to, codes or public cryptographic keys) which are used for the purpose of verifying an electronic signature;

“signature-verification device” means configured software or hardware used to implement the signature-verification data;

“voluntary accreditation” means any permission, setting out rights and obligations specific to the provision of certification services, to be granted upon request by the certification-service-provider concerned by the person charged with the elaboration of, and supervision of

(1) OJNo. L13, 19.1.00, p. 12.

compliance with, such rights and obligations, where the certification-service-provider is not entitled to exercise the rights stemming from the permission until he has received the decision of that person.

Supervision of certification-service-providers

3.—(1) It shall be the duty of the Secretary of State to keep under review the carrying on of activities of certification-service-providers who are established in the United Kingdom and who issue qualified certificates to the public and the persons by whom they are carried on with a view to her becoming aware of the identity of those persons and the circumstances relating to the carrying on of those activities.

(2) It shall also be the duty of the Secretary of State to establish and maintain a register of certification-service-providers who are established in the United Kingdom and who issue qualified certificates to the public.

(3) The Secretary of State shall record in the register the names and addresses of those certification-service-providers of whom she is aware who are established in the United Kingdom and who issue qualified certificates to the public.

(4) The Secretary of State shall publish the register in such manner as she considers appropriate.

(5) The Secretary of State shall have regard to evidence becoming available to her with respect to any course of conduct of a certification-service-provider who is established in the United Kingdom and who issues qualified certificates to the public and which appears to her to be conduct detrimental to the interests of those persons who use or rely on those certificates with a view to making any of this evidence as she considers expedient available to the public in such manner as she considers appropriate.

Liability of certification-service-providers

4.—(1) Where—

(a) a certification-service-provider either—

- (i) issues a certificate as a qualified certificate to the public, or
- (ii) guarantees a qualified certificate to the public,

(b) a person reasonably relies on that certificate for any of the following matters—

- (i) the accuracy of any of the information contained in the qualified certificate at the time of issue,
- (ii) the inclusion in the qualified certificate of all the details referred to in Schedule 1,
- (iii) the holding by the signatory identified in the qualified certificate at the time of its issue of the signature-creation data corresponding to the signature-verification data given or identified in the certificate, or
- (iv) the ability of the signature-creation data and the signature-verification data to be used in a complementary manner in cases where the certification-service-provider generates them both,

(c) that person suffers loss as a result of such reliance, and

(d) the certification-service-provider would be liable in damages in respect of any extent of the loss—

- (i) had a duty of care existed between him and the person referred to in subparagraph (b) above, and
- (ii) had the certification-service-provider been negligent,

then that certification-service-provider shall be so liable to the same extent notwithstanding that there is no proof that the certification-service-provider was negligent unless the certification-service-provider proves that he was not negligent.

(2) For the purposes of the certification-service-provider's liability under paragraph (1) above there shall be a duty of care between that certification-service-provider and the person referred to in paragraph (1)(b) above.

(3) Where—

- (a) a certification-service-provider issues a certificate as a qualified certificate to the public,
- (b) a person reasonably relies on that certificate,
- (c) that person suffers loss as a result of any failure by the certification-service-provider to register revocation of the certificate, and
- (d) the certification-service-provider would be liable in damages in respect of any extent of the loss—
 - (i) had a duty of care existed between him and the person referred to in sub-paragraph (b) above, and
 - (ii) had the certification-service-provider been negligent,

then that certification-service-provider shall be so liable to the same extent notwithstanding that there is no proof that the certification-service-provider was negligent unless the certification-service-provider proves that he was not negligent.

(4) For the purposes of the certification-service-provider's liability under paragraph (3) above there shall be a duty of care between that certification-service-provider and the person referred to in paragraph (3)(b) above.

Data Protection

5.—(1) A certification-service-provider who issues a certificate to the public and to whom this paragraph applies in accordance with paragraph (6) below—

- (a) shall not obtain personal data for the purpose of issuing or maintaining that certificate otherwise than directly from the data subject or after the explicit consent of the data subject, and
- (b) shall not process the personal data referred to in sub-paragraph (a) above—
 - (i) to a greater extent than is necessary for the purpose of issuing or maintaining that certificate, or
 - (ii) to a greater extent than is necessary for any other purpose to which the data subject has explicitly consented,

unless the processing is necessary for compliance with any legal obligation, to which the certification-service-provider is subject, other than an obligation imposed by contract.

(2) The obligation to comply with paragraph (1) above shall be a duty owed to any data subject who may be affected by a contravention of paragraph (1).

(3) Where a duty is owed by virtue of paragraph (2) above to any data subject, any breach of that duty which causes that data subject to sustain loss or damage shall be actionable by him.

(4) Compliance with paragraph (1) above shall also be enforceable by civil proceedings brought by the Crown for an injunction or for an interdict or for any other appropriate relief or remedy.

(5) Paragraph (4) above shall not prejudice any right that a data subject may have by virtue of paragraph (3) above to bring civil proceedings for the contravention or apprehended contravention of paragraph (1) above.

(6) Paragraph (1) above applies to a certification-service-provider in respect of personal data only if the certification-service-provider is established in the United Kingdom and the personal data are processed in the context of that establishment.

(7) For the purposes of paragraph (6) above, each of the following is to be treated as established in the United Kingdom—

- (a) an individual who is ordinarily resident in the United Kingdom,
- (b) a body incorporated under the law of, or in any part of, the United Kingdom,
- (c) a partnership or other unincorporated association formed under the law of any part of the United Kingdom, and
- (d) any person who does not fall within sub-paragraph (a), (b) or (c) above but maintains in the United Kingdom—
 - (i) an office, branch or agency through which he carries on any activity, or
 - (ii) a regular practice.

(8) In this regulation—

“data subject” and “personal data” and “processing” shall have the same meanings as in section 1(1) of the Data Protection Act 1998⁽²⁾, and

“obtain” shall bear the same interpretation as “obtaining” in section 1(2) of the Data Protection Act 1998.

Douglas Alexander
Minister of E-Commerce and Competitiveness in
Europe,
Department of Trade and Industry

13th February 2002

(2) 1998 c. 29.