
STATUTORY INSTRUMENTS

2017 No. 692

The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017

PART 4

Reliance and Record-keeping

Record-keeping

40.—(1) Subject to paragraph (5), a relevant person must keep the records specified in paragraph (2) for at least the period specified in paragraph (3).

(2) The records are—

(a) a copy of any documents and information obtained by the relevant person to satisfy the customer due diligence requirements in regulations 28, 29 and 33 to 37 [^{F1}and the requirements of regulation 30A]^{F2}, and of regulations 64C and 64G(1);

(b) sufficient supporting records (consisting of the original documents or copies) in respect of a transaction (whether or not the transaction is an occasional transaction) which is the subject of customer due diligence measures or ongoing monitoring to enable the transaction to be reconstructed.

[^{F3}(c) in the case of an inter-cryptoasset business transfer, in addition to the records referred to in sub-paragraphs (a) and (b), any documents and information received by an intermediary cryptoasset business and the cryptoasset business of a beneficiary by virtue of the obligations under regulations 64C(1), (2) and (7), or received by them pursuant to a request under regulation 64D(2)(a) or 64E(2)(a); and

(d) in the case of an unhosted wallet transfer, in addition to the records referred to in sub-paragraphs (a) and (b), any documents and information received by a cryptoasset business pursuant to a request under regulation 64G(1).]

(3) Subject to paragraph (4), the period is five years beginning on the date on which the relevant person knows, or has reasonable grounds to believe—

(a) that the transaction is complete, for records relating to an occasional transaction; or

(b) that the business relationship has come to an end for records relating to—

(i) any transaction which occurs as part of a business relationship, or

(ii) customer due diligence measures taken in connection with that relationship.

(4) A relevant person is not required to keep the records referred to in paragraph (3)(b)(i) for more than 10 years.

(5) Once the period referred to in paragraph (3), or if applicable paragraph (4), has expired, the relevant person must delete any personal data obtained for the purposes of these Regulations unless—

(a) the relevant person is required to retain records containing personal data—

- (i) by or under any enactment, or
 - (ii) for the purposes of any court proceedings;
 - (b) the data subject has given consent to the retention of that data; or
 - (c) the relevant person has reasonable grounds for believing that records containing the personal data need to be retained for the purpose of legal proceedings.
- (6) A relevant person who is relied on by another person must keep the records specified in paragraph (2) for the period referred to in paragraph (3) or, if applicable, paragraph (4).
- (7) A person referred to in regulation 39(3) (“A”) who is relied on by a relevant person (“B”) must, if requested by B within the period referred to in paragraph (3) or, if applicable, paragraph (4), immediately—
- (a) make available to B any information about the customer, any person purporting to act on behalf of the customer and any beneficial owner of the customer, which A obtained when applying customer due diligence measures; and
 - (b) forward to B copies of any identification and verification data and other relevant documents on the identity of the customer, any person purporting to act on behalf of the customer and any beneficial owner of the customer, which A obtained when applying those measures.
- (8) Paragraph (7) does not apply where a relevant person applies customer due diligence measures by means of an agent or an outsourcing service provider (within the meaning of regulation 39(8)).
- (9) For the purposes of this regulation—
- (a) B relies on A where B does so in accordance with regulation 39(1);
 - (b) “copy” means a copy of the original document which would be admissible as evidence of the original document in court proceedings;
 - [^{F4}(c) “data subject” has the same meaning as in the Data Protection Act 2018 (see section 3 of that Act);
 - (d) “personal data” has the same meaning as in Parts 5 to 7 of that Act (see section 3(2) and (14) of that Act).]
 - [^{F5}(e) “beneficiary”, “cryptoasset business”, “inter-cryptoasset business transfer”, “intermediary cryptoasset business” and “unhosted wallet transfer” have the meanings given by regulation 64B.]

Textual Amendments

- F1** Words in reg. 40(2)(a) inserted (6.10.2020) by The Money Laundering and Terrorist Financing (Amendment) (EU Exit) Regulations 2020 (S.I. 2020/991), regs. 1(2), **4(4)**
- F2** Words in reg. 40(2)(a) inserted (1.9.2023) by The Money Laundering and Terrorist Financing (Amendment) (No. 2) Regulations 2022 (S.I. 2022/860), regs. 1(3), **5(4)(a)**
- F3** Reg. 40(2)(c)(d) inserted (1.9.2023) by The Money Laundering and Terrorist Financing (Amendment) (No. 2) Regulations 2022 (S.I. 2022/860), regs. 1(3), **5(4)(b)**
- F4** Reg. 40(9)(c)(d) substituted for reg. 40(9)(c) (25.5.2018) by Data Protection Act 2018 (c. 12), s. 212(1), **Sch. 19 para. 414** (with ss. 117, 209, 210); S.I. 2018/625, reg. 2(1)(g)
- F5** Reg. 40(9)(e) inserted (1.9.2023) by The Money Laundering and Terrorist Financing (Amendment) (No. 2) Regulations 2022 (S.I. 2022/860), regs. 1(3), **5(4)(c)**

Changes to legislation:

There are currently no known outstanding effects for the The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, Section 40.