trustcorp

trustseed

PORTAL OF DIGITAL SERVICES

COMPLIANCE WITH REGULATIONS GDPR-E.IDAS-NIS
UNIVERSAL SOLUTION OF ENTERPRISE

TRUSTSEED SAS | STUDY OF DIGITAL TRANSFORMATION | August 13. 2018

trustseed

SERVICE OFFER on the PORTAL

Here are the 10 mandatory services on an Internet portal under the new GDPR, e.IDAS and NIS (Network Information Security) regulations. These services comply with the following regulatory arsenal:

1. The GDPR Regulation now separates the responsibilities for the one hand, the "services" to the customers including the offer and the complete protection of their personal data (before and after treatment), and on the other hand, the operations requiring a "Qualified provider" to create originals of documents and signatures as well as to encrypt (confidentiality) and transmit (integrity) the files.

2. The GDPR regulation also imposes in the relations between the legal persons of the same community, including their employees (Binding Corporate Rules Art.47), and for the transfers of personal data (Art.48), to respect the "appropriate guarantees" (Art.24.1 and 25.1.2) and the "reporting mechanisms" (Art.40.4 and 41.2.b) defined by the supervisory authority or its delegate, an approved inspection body responsible for the application of the Community Code of Conduct. These "guarantees" and these "mechanisms" are based on reliable computer means to be certified also (Art.25.3 and 42.6.7) .They allow, in compliance with the code of conduct, to ensure the legal and electronic security of the mails, transactions and means of payment both at the level of the users and at the level of the employees in the internal organization.

The service manager on his Internet portal must absolutely determine the purposes and means of treatment for each type of mail, transaction or payment; and as such, he is the first responsible for "technical and organizational measures" (Art.24) that must be implemented for each request of a "data subject", ie a user.

3. The e.IDAS Regulation imposes in this context legal identification, authentication, signature and consent schemes, as well as security rules to ensure the integrity and timestamping of files with electronic seals; the e.IDAS regulation, like the GDPR regulation, also imposes validation rules to ensure the independence of the identity and authentication controls of conformity ("no one can constitute proof to itself"): revocation lists and special rights (claim, opposition, rectification, pseudonymisation, portability) have to be verified in real time for each account holder.

4. The NIS Directive imposes safety standards on the Communities to ensure the interoperability of trade in trust and the resilience of procedures.

Here is the list of services and functions that should be installed on a "portal" to comply (Solidarity Penalty Art 83 a, b, c), to be interoperable with other portals (Companies, Communities or Administrations and Subcontractors) and to possibly benefit from the labels CE.

SERVICES AND FUNCTIONS OF THE INTERNET PORTAL

1. Access to the Portal for opening an account (Qualified Certificate of Website Authentication Article 45. E.IDAS), Registrar.

2. Account holder's access to the Portal, management of the strong authentication means (Article 3.6.7.8).

3. Download credentials, handwritten signature fingerprint and documentary and banking secrets (IBAN).

4. Services:

    a. Procedures - administrative forms

    b. Mail:

        i. Notarized Email

        ii. Registered letter AR digital (Art 44 - 46 e.IDAS)

    c. Contract signed bi or multilateral

    d. Standard invoice unilateral signature

    e. Payment :

        i. By Card

        ii. Direct Debit (PSD2)

        iii. QR Code payment

    f. Other.

5. Management of signing proxies

   a. For administrative procedures

   b. For letters

   c. For contracts

   d. For payments

   e. For the Others

6. Counterparty management

   a. invitations

   b. Signature of bilateral conventions

7. Certificate Management

   a. Qualified Portal Authentication Certificates

   b. Advanced Signing Certificates (Multiple Signatories)

   c. Encryption Certificates (Account and Document)

8. Management of Auxiliary Rights:

   a. Claim procedure

   b. Opposition procedure

   c. Pseudonymisation procedure

   d. Rectification procedure

   e. Clearing procedure

   f. Portability procedure

   g. Procedure for consulting the records of traceability

9. Management of the encrypted documentary current account

10. Rule Management by Document Types

- a. Life cycle of the document
- b. Traceability record and registers.

USUAL ELECTRONIC COMMITMENT BY SIGNATURE "OFF LINE"

BEFORE CHANGE OF METHODOLOGY AND STANDARDS : PORTAL SERVICES

EXCHANGE FINALISATION Final Destination	TREATMENT LIMITATION (OPERATIONS)	DATA MINIMIZATION (Files & Data COLLECTION)	SOFTWARE TRACEABILITY MECHANISM CONFORMITY	RESPONS ABILITY	APPROPRIATE TECHNICAL OR ORGANISATIONAL MEASURES SEQUENCES USER= 10 Functions (72 %) Processor- Operator = 4 Functions (28%)	SPEED EXEC LOW Normal LATE	VALIDATION By the User Himself Evidence Value Low, substantial and high
		x	LOW	USER	1.Identity management	LOW	L
		X	LOW	USER	2.Secret management - marking of stored personal data	LOW	L
		X	LOW	USER	3.Commitment management + Options	LOW	L
	x		LOW	USER	4.Powers management multilateral	LOW	L
	x	x	LOW	USER	5.Counterparty management multilateral	LOW	L
	x		LOW	USER	6.Keys control management	LOW	L
		x	Substantial	USER	7.ID Identification - Authentication Mechanisms Multilateral	N	S
		x	Substantial	USER	8.Data Files Collection Consent	N	S
	x	x	LOW	USER	9.Originals Document Creation Multilateral Mechanism Cross Border	LOW	L
	x		LOW	Processor	10.Originals Signature Creation Low Multilateral Mechanism	N	L
		x	LOW	USER	11.Strong Consent Management Multilateral Mechanism Cross Border	LOW	L
x			LOW	Processor	12.Communication of management information Multilateral Mechanism Low encryption low secrecy.	LOW	L
x			LOW	Processor	13.Transfer of legal proof Archiving Low encryption & secrecy.	LOW	L
x			LOW	USER	14.Switch of Ownership -Accounting Low encryption Low secrecy.	LOW	L
			LOW	USER	Option Right to compensation and liability	LATE	L
			LOW	USER	Option Right to object, to pseudonymize	LATE	L
			LOW	USER	Option Right to revoke, to rectify, to **erasure & to use data portability**	LATE	L
			LOW	USER	Low Control of profiling by automated processing	LATE	L
			LOW	USER	Low Control of Mandatory archiving, scientific, historical research or statistical purposes by automated processing	LATE	L
			LOW	USER	Without Control of Mandatory letters rogatory or judicial warrants by automated processing	LATE	L

MANDATORY APPROPRIATE OR SUITABLE SAFEGUARDS 1

IT SOFTWARES & DEVICES CERTIFICATION

'Electronic identification scheme', hardware or software, or relevant components of hardware or software, which are intended to be used for the provision of trust services:

(g) 'qualified certificate for website authentication',
(h) 'electronic Commitment by signature scheduling'
(i) 'electronic document file origination or creation device',
(j) 'electronic signature creation device', 'electronic seal creation device', 'electronic timestamp creation device'
(k) 'electronic registered delivery service',
(l) 'validation device ' the process of verifying and confirming that an electronic document, signature - consent or a seal, all of them including traceability control mechanisms is valid.

RISK

MGT

MANDATORY APPROPRIATE OR SUITABLE SAFEGUARDS 2

TRUST SERVICE CODE OF CONDUCT

'trust service' means an electronic service normally provided for remuneration which consists of:

(a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or

(b) the creation, verification and validation of certificates for website authentication; or

(c) the preservation of electronic signatures, seals or certificates related to those services;

UNIVERSAL MANAGEMENT OF DIGITAL COMMITMENTS BY SIGNATURE IN CLOUD COMPUTING

COMPLIANT WITH GDPR REGULATION : PORTAL SERVICES

EXCHANGE FINALISATION Final Destination	TREATMENT LIMITATION (OPERATIONS)	DATA MINIMIZATION (Files & Data COLLECTION)	CONFORMITY ASSESSMENT BODY Art.42-43 3years Mechanism	RESPONS ABILITY	APPROPRIATE TECHNICAL OR ORGANISATIONAL MEASURES- SEQUENCES USER= 3 FUNCTIONS (21%) CONTROLLER = 6 FUNCTIONS (43 %) PROCESSOR = 5 FUNCTIONS (36 %)	SPEED EXEC Real Time	VALIDATION BODY GUARANTEES Art.40 & 41 CONTROL MECHANISMS
		x	Certification 1	Controller	Identity management	RT	BLOCKCHAIN 1 SEAL INTEGRITY TIMESTAMP CERTIFICATION SIGNATURE
		x	Certification 2	Controller	Secret management - marking of stored personal data	RT	
x	x	x	Certification 3	Controller	Commitment management + Options 15 - 16 -17 .	RT	
	x		Certification 4	Controller	Powers management multilateral	RT	
	x		Certification 5	Controller	Counterparty management multilateral	RT	
			Certification 6	Controller	Keys control mechanism multilateral	RT	
			Certification 7	USER	ID Identification - Authentication Mechanisms Multilateral	RT	
			Certification 8	USER	Data Files Collection Consent	RT	BLOCKCHAIN 2 SEAL INTEGRITY TIMESTAMP SIGNATURE CERTIFICATION GUARANTEE
	x	x	Certification 9	Processor	Originals Document Creation Multilateral Mechanism Cross Border	RT	
	x		Certification 10	Processor	Originals Signature Creation Multilateral Mechanism Cross Border	RT	
			Certification 11	USER	Strong Consent Management Multilateral Mechanism Cross Border	RT	
x			Certification 12	Processor	Communication of management information Multilateral Mechanism Encryption Statutory obligation of secrecy.	RT	
x			Certification 13	Processor	Transfer of legal Accounting-Archiving Multilateral Mechanism Encryption Statutory obligation of secrecy.	RT	
x			Certification 14	Processor	Switch of Ownership Multilateral Mechanism Encryption Statutory obligation of secrecy.	RT	
x			Certification 15	15	Option Right to compensation and liability	RT	SPECIFIC BLOCKCHAINS SEAL INTEGRITY TIMESTAMP CERTIFICATION SIGNATURE
x			Certification 16	16	Option Right to object, to pseudonymize	RT	
x			Certification 17	17	Option Right to revoke, to rectify, to **erasure & to use data portability**	RT	
x		x	Certification 18	18	Controlled Acceptance of profiling by automated processing	RT	
x		x	Certification 19	19	Controlled Mandatory archiving, scientific, historical research or statistical purposes by automated processing	RT	
x		x	Certification 20	20	Controlled Mandatory letters rogatory or judicial warrants by automated processing	RT	

MANDATORY APPROPRIATE OR SUITABLE SAFEGUARDS 1

IT SOFTWARES & DEVICES CERTIFICATION

Certificat

'Electronic identification scheme', hardware or software, or relevant components of hardware or software, which are intended to be used for the provision of trust services:

(a) 'qualified certificate for website authentication',
(b) 'electronic Commitment by signature scheduling'
(c) 'electronic document file origination or creation device',
(d) 'electronic signature creation device', 'electronic seal creation device', 'electronic timestamp creation device'
(e) 'electronic registered delivery service',
(f) 'validation device ' the process of verifying and confirming that an electronic document, signature - consent or a seal, all of them including traceability control mechanisms is valid.

RISK

MGT

MANDATORY APPROPRIATE OR SUITABLE SAFEGUARDS 2

TRUST SERVICE CODE OF CONDUCT

Certificat

'trust service' means an electronic service normally provided for remuneration which consists of:

(a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or

(b) the creation, verification and validation of certificates for website authentication; or

(c) the preservation of electronic signatures, seals or certificates related to those services;