Bill Number:

DIGITAL IDENTITY BILL

DIGITAL IDENTITY BILL

Bill sponsored by

Date:

Reason for Submission of Bill

The reason for submission of this Bill by the Government is to formulate an enabling legal framework for digital identities in the Maldives and to establish the principles, responsibilities, processes, coordination mechanisms and functions to govern the implementation and operation of the Maldives Digital Identity System in order to facilitate the ability of citizens and residents to authenticate their identities and engage in online transactions.

_____

Member submitting the Bill on behalf of the Government:

DIGITAL IDENTITY BILL

CHAPTER 1 **PREAMBLE**			
Introduction and Title	**1.**	(a)	This Act provides for the principles to govern the implementation of the Maldives Digital Identity System to promote digital transformation, facilitate the use of digital identities and foster the use of online services in the Maldives.
		(b)	This Act may be cited as the "Digital Identity Act".
Objectives	**2.**	The objectives of this Act are:	
		(a)	to provide eligible persons with unique, secure, convenient, voluntary, legally recognized and inclusive ways to authenticate their identity in online transactions and in in-person verification with public agencies, legal entities or other persons;
		(b)	to promote privacy and the security of identity information used to authenticate the identity or attributes of registered persons;
		(c)	to facilitate economic benefits for, and reduce burdens on, the Maldivian economy by encouraging the use of digital identity and online services;
		(d)	to promote trust in digital identities within Maldivian society; and
		(e)	to provide consideration for the future of digital identities, having regard for rapid changes in technology, international standards and the evolving threat environment.
Application	**3.**	This Act applies to the following areas and activities:	

		(a)	the territory or the Maldives and outside the territory of the Maldives for citizens living abroad and other persons applying for legal permits to reside in the Maldives; and
		(b)	all activities relating to digital identity functions.
Legal validity and status of digital identity, Maldives Digital Identity Numbers, etc.	**4.**	(a)	Where a registered person is required by law or regulation to produce evidence of their identity, the production of a Maldives Digital Identity Number, an associated token or an authenticator must be accepted as sufficient proof of identity for that purpose, subject to authentication under this Act.
		(b)	Where any law or regulation requires the retention of evidence of proof of identity presented at the time of a transaction, the storage of cryptographically verifiable metadata associated with the presentation of a Maldives Digital Identity Number, an associated token, or an authenticator is deemed to satisfy that requirement, provided such cryptographic evidence meets the requirements and standards set forth by regulation.
		(c)	Nothing in this Act requires or prevents an eligible person:
		(1)	to register with the Maldives Digital Identity System in accordance with section **Error! Reference source not found.**15 and to obtain a Maldives Digital Identity Number or associated token in accordance with section 18; or
		(2)	to use a Maldives Digital Identity Number, associated token, digital wallet or authenticator assigned to him or her to use, acquire or access a service offered by a relying party.
		(d)	A registered person may continue to use, acquire or access a service offered by a relying party by means other than by using a Maldives Digital Identity Number or associated tokens or digital wallet or authenticator for identity authentication, even if a Maldives Digital Identity Number or associated token or digital wallet or authenticator has been assigned or approved to such registered person.

CHAPTER 2 **THE MALDIVES DIGITAL IDENTITY SYSTEM**			
The Maldives Digital Identity System	**5.**	(a)	The Maldives Digital Identity System is hereby established to operationalize digital identity registration and authentication in the Republic of Maldives.
		(b)	The Maldives Digital Identity System is comprised of:
		(1)	the following electronic databases established in the Maldives which will serve as the foundational identity databases for the Maldives Digital Identity System:
		(i)	the national identity card registration system;
		(ii)	the work permit registration system; and
		(iii)	the visa registration system; and
		(2)	the MDIDS database addressed in section 12**Error! Reference source not found.**; and
		(3)	the associated systems and platforms deployed by the MDIDS Administrator to implement the MDIDS database and operationalize the registration and authentication functions established in this Act.
		(c)	The databases and systems that integrate the Maldives Digital Identity System must be designed and administered in accordance with generally accepted international standards to ensure security, accuracy, integrity and currency of identity information and must be interoperable in accordance with the requirements of section 14.
Participating parties in the Maldives Digital Identity System	**6.**	The following are the public agencies, legal entities and persons participating in the Maldives Digital Identity System:	
		(a)	the Minister;
		(b)	the MDIDS Administrator;
		(c)	identity information providers;
		(d)	relying parties; and

		(e)	registered persons.
Roles of the Minister within the Maldives Digital Identity System	**7.**	The Minister has the following roles and responsibilities under this Act:	
		(a)	overseeing the Maldives Digital Identity System to ensure compliance with national security considerations;
		(b)	overseeing the MDIDS Administrator's effective compliance with its roles and responsibilities under this Act;
		(c)	promoting cooperation, consultation and collaboration among the MDIDS Administrator, identity information providers and relying parties to facilitate the effective implementation of the Maldives Digital Identity System;
		(d)	fostering public confidence and trust in the Maldives Digital Identity System to enhance registration of eligible persons in the Maldives Digital Identity System;
		(e)	promoting the increased use of, and participation in, the Maldives Digital Identity System of public agencies, legal entities and other persons as relying parties;
		(f)	making regulations as required under this Act; and
		(g)	issuing written directions to the MDIDS Administrator to do any of the following things based on national security considerations:
		(1)	to refuse to approve the participation of a public agency, legal entity or person as a relying party in the Maldives Digital Identity System;
		(2)	to suspend the approval of participation of a public agency, legal entity or person as a relying party in the Maldives Digital Identity System; or
		(3)	to cancel the approval of participation of a public agency, legal entity or person as a relying party in the Maldives Digital Identity System.
The MDIDS Administrator	**8.**	(a)	The MDIDS Administrator is responsible for the following functions under this Act:

		(1)	registering eligible persons in the Maldives Digital Identity System and assigning Maldives Digital Identity Numbers and associated tokens, as applicable;
		(2)	discharging the authentication function of the Maldives Digital Identity System under this Act;
		(3)	managing the operations and technical design of the MDIDS database and the associated platforms and systems to implement the Maldives Digital Identity System, directly or through third parties;
		(4)	approving digital wallets and issuing or authorizing third parties to issue verifiable credentials under this Act;
		(5)	assisting parties participating in the Maldives Digital Identity System, including in relation to connecting to, and addressing incidents involving the Maldives Digital Identity System;
		(6)	promptly responding to queries and grievances logged by registered persons in accordance with this Act;
		(7)	facilitating and monitoring the use of the Maldives Digital Identity System for testing purposes in accordance with any requirements prescribed in applicable regulations;
		(8)	monitoring and managing the availability of the Maldives Digital Identity System, including system upgrades, changes and outages;
		(9)	identifying, managing and resolving systemic issues and operational risks relating to the performance and integrity of the Maldives Digital Identity System;
		(10)	maintaining the accuracy, relevance, integrity, timeliness, privacy, security and professional standards in relation to identity information processed by the Maldives Digital Identity System;
		(11)	managing digital identity fraud incidents and cyber security incidents involving entities participating in the Maldives Digital Identity System;

		(12)	advising the Minister, either on its own initiative or on request, on matters relating to the Maldives Digital Identity System;
		(13)	implementing directions issued by the Minister;
		(14)	coordinating with the Data Protection Authority, either on its own initiative or on request, on personal data protection matters pertaining to the Maldives Digital Identity System;
		(15)	coordinating with the National Cyber Security Agency, either on its own initiative or on request, on cybersecurity matters pertaining to the Maldives Digital Identity System;
		(16)	undertaking audits of the Maldives Digital Identity System and relying parties in accordance with this Act;
		(17)	making regulations as required to implement this Act;
		(18)	exercising such other functions as are conferred on the MDIDS Administrator by this Act or any other law; and
		(19)	doing anything that is necessary, incidental or conducive to the performance of any of the above functions.
	(b)		The MDIDS Administrator must publish on its website an annual report on the performance of the Maldives Digital Identity System which must include at least the following information:
		(1)	a description of the level of registration of eligible persons in the Maldives Digital Identity System at the national level and by atoll;
		(2)	a description of the relying parties active in the Maldives Digital Identity System;
		(3)	a description of the level of use of the Maldives Digital Identity System;
		(4)	high-level description of data security and privacy safeguards of the Maldives Digital Identity System; and
		(5)	a description of the costs of the Maldives Digital Identity System and fees collected under this Act.

	(c)		The MDIDS Administrator will not be liable to any person, relying party or other third party for any loss or damages resulting from:
		(1)	any malfunction of the Maldives Digital Identity System; or
		(2)	any human error; or
		(3)	an incorrect verification or authentication of a registered person;
			provided that such loss or damage is not committed in bad faith or the result of willful misconduct or gross negligence.
Identity information providers	**9.**	(a)	The following public agencies are hereby designated as identity information providers within the Maldives Digital Identity System:
		(1)	the Department of National Registration, or the public agency entrusted with the responsibility for developing and managing the national identity card registration system from time to time;
		(2)	the public agency entrusted with the responsibility for developing and managing the work permit registration system for residents from time to time; and
		(3)	the public agency entrusted with the responsibility for developing and managing the visa registration system for residents from time to time.
		(b)	The identity information providers must:
		(1)	establish technical and organizational coordination mechanisms with the MDIDS Administrator to facilitate implementation of this Act;
		(2)	enter into data sharing agreements with the MDIDS Administrator to facilitate the registration and authentication functions established in this Act; and
		(3)	maintain the accuracy, integrity, privacy, and security of the databases they manage in a manner consistent with internationally recognized standards and applicable laws.

Relying parties	**10.**	(a)	Relying parties may seek access to the authentication function of the Maldives Digital Identity System in order to:
		(1)	provide a good or service to a registered person; or
		(2)	enable a registered person to access a good or service.
		(b)	A public agency, legal entity and other person seeking to act as a relying party must:
		(1)	apply for appointment by the MDIDS Administrator as a relying party in the manner prescribed by the MDIDS Administrator;
		(2)	specify to the MDIDS Administrator the reasons for and nature of the access they seek to the authentication function of the Maldives Digital Identity System;
		(3)	provide such information as is required by the MDIDS Administrator or by regulation to determine whether the applicant should be appointed as a relying party; and
		(4)	demonstrate to the satisfaction of the MDIDS Administrator that the applicant has implemented the necessary policies and procedures and has administrative and technical capacity and readiness to assume the responsibilities and obligations of a relying party under this Act and any applicable regulations.
		(c)	Upon verification of the application and accompanying documentation submitted in accordance with subsection (b), the MDIDS Administrator may:
		(1)	approve the application received; and
		(2)	enter into relevant agreements with the applicant which must incorporate the terms and conditions for use by the relying party of the authentication function, including privacy and security protections, technical requirements, and penalties for non-performance of obligations.

		(d)	If the MDIDS Administrator is of the view that an application for appointment as a relying party does not satisfy the qualification requirements specified in this Act or in regulation, the MDIDS Administrator may reject the application and communicate its decision to the applicant in the manner prescribed in regulation.
		(e)	Relying parties must submit reports to, and promptly respond to information requests from, the MDIDS Administrator regarding compliance with the obligations set forth in this Act and its regulations.
		(f)	Relying parties must comply with directions issued by the MDIDS Administrator under this Act.
		(g)	The MDIDS Administrator:
		(1)	must publish an updated list of all active relying parties on the Maldives Digital Identity System website or in such other manner as the MDIDS Administrator deems necessary;
		(2)	may issue written directions to relying parties to ensure compliance with obligations set forth under this Act and its regulations;
		(3)	may make regulations specifying roles and responsibilities for relying parties; and
		(4)	may suspend or cancel a relying party's participation in the Maldives Digital Identity System in accordance with the processes and requirements prescribed by regulation.
Registered persons	**11.**	(a)	A registered person may consent to authenticate his or her identity through the Maldives Digital Identity System to use, acquire or access goods or services offered by a relying party.
		(b)	A registered person has the right to obtain from the MDIDS Administrator or from a relying party, promptly and without constraint:
		(1)	confirmation as to whether or not the MDIDS Administrator or a data processor acting on its behalf is storing or otherwise processing identity information relating to the individual;

		(2)	confirmation as to whether a relying party or a data processor acting on its behalf is storing or otherwise processing his or her identity information obtained from the Maldives Digital Identity System;
		(3)	a copy of such identity information in a commonly used digital format;
		(4)	correction of any such identity information that is inaccurate, out of date, or incomplete; and
		(5)	deletion of any such identity information or personal data which the Maldives Digital Identity System, or the relying party, or a data processor, is not permitted to process under this Act.
		(c)	The MDIDS Administrator and relying parties must implement measures necessary to ensure that a registered person is able to effectively exercise the rights set out in subsection (b).
		(d)	Notwithstanding the generality of subsection (c), the MDIDS Administrator may make regulations exempting or allowing the waiver of specific requirements under this section for specific categories of relying parties on account of their scale and availability of resources, among other matters, provided that a relying party must notify registered persons at the time of authentication of the exemptions and/or waivers that apply to such relying party.
CHAPTER 3 **MDIDS DATABASE**			
The MDIDS database	**12.**	(a)	The MDIDS Administrator must, directly or through engagement of one or more third parties, develop, upgrade and maintain such databases and associated systems and platforms as are necessary to implement this Act to be known as the MDIDS database.

		(b)	The MDIDS database has the purpose of enabling identification and authentication of registered persons in accordance with this Act and must:
		(1)	separately store biographic information and biometric information obtained from the registration process undertaken in accordance with section 15 and such other sources as may be prescribed by regulation;
		(2)	be designed and managed to be compliant with generally accepted international standards on data security, integrity and confidentiality;
		(3)	be effectively linked to, and be capable of retrieving, extracting, querying and caching identification information from, the foundational identity databases identified in section 5(b)(1); and
		(4)	be stored on servers located within data centers located in the Maldives, while failover systems or back-ups may be stored in other countries.
		(c)	For avoidance of doubt, the MDIDS database and associated systems and platforms referred to in subsection (a) do not substitute or replace the databases identified in section 5(b)(1) which will remain the foundational identity databases within the Maldives Digital Identity System.
		(d)	The MDIDS Administrator must ensure mechanisms and processes are in place such that information stored in the MDIDS database is accurate and current in relation to the foundational identity databases identified in section 5(b)(1).
Update and correction of certain information	**13.**	(a)	The MDIDS Administrator may require registered persons to update their biographic information and biometric information, from time to time, in such manner as may be specified by regulations.

		(b)	The MDIDS Administrator must provide an easily accessible means for registered persons to correct and update biographic information and biometric information about themselves stored in the MDIDS database that is not current, complete or accurate.
		(c)	Failure to update information pursuant to a requirement under subsection (a) will not on its own result in the deactivation of the registered person's Maldives Digital Identity Number or authenticator.
Interoperability of identity databases and data sharing	**14.**	(a)	The MDIDS Administrator and the identity information providers must enter into agreements and put in place effective mechanisms to ensure the secure interoperability among the MDIDS database, the national identity card registration system, the work permit registration system and the visa registration system.
		(b)	The purpose of interoperability requirements under subsection (a) are:
		(1)	to enable the MDIDS database to access authoritative information about an eligible person held in the national identity card registration system, the work permit registration system and the visa registration system to support the complete and accurate registration of such person in accordance with section 15;
		(2)	to facilitate the performance of the authentication function in accordance with section **Error! Reference source not found.**;
		(3)	to enable the use of biographic data of a registered person held in the MDIDS database to update and maintain accurate, as warranted, the national identity card registration system, the work permit registration system and the visa registration system; and
		(4)	to record and use a registered person's Maldives Digital Identity Number or associated tokens in the national identity card registration system, the work permit registration system and the visa registration system, as warranted.

		(c)	Access to and sharing of information between databases under subsection (a) must be restricted to the purposes provided in subsection (b) and such other ancillary purposes as may be prescribed in regulation, provided that in no case identity information may be shared for commercial purposes, including but not limited to direct marketing.
		(d)	Interoperability of databases and data sharing of information undertaken in accordance with this section must be done in a manner that fully complies with generally accepted international standards to ensure data security, privacy, integrity and confidentiality.
CHAPTER 4 **REGISTRATION**			
Registration requirements	**15.**	(a)	Every eligible person is entitled to register with the Maldives Digital Identity System by filing an application in the manner prescribed by the MDIDS Administrator.
		(b)	For the purpose of registration, eligible persons must submit the following biographic and biometric:
		(1)	Biographic information:
		(i)	name;
		(ii)	national identity number, work permit number or passport number, as applicable;
		(iii)	date of birth
		(iv)	place of birth;
		(v)	gender;
		(vi)	permanent address;
		(vii)	current address;
		(viii)	mobile phone number, as applicable;
		(ix)	email address, as applicable; and
		(x)	such additional biographic information as may be determined by regulation.
		(2)	Biometric information:
		(i)	facial image; and

		(ii)	such additional biometric information as may be determined by regulation.
		(c)	A representative may initiate the registration process by acting on behalf of an eligible person by filing an application in the manner prescribed by the MDIDS Administrator and must provide the following information in addition to that described in subsection (b):
		(1)	name of the representative;
		(2)	relationship or representation with the applicant;
		(3)	national identity number, work permit number or passport number of the representative, as applicable;
		(4)	facial image of the representative; and
		(5)	such additional information as may be determined by regulation.
		(d)	The MDIDS Administrator must, at the time of registration, inform the eligible person undergoing registration of the following:
		(1)	the manner and purpose for which the identity information collected will be used;
		(2)	the recipients with whom the identity information collected is intended to be shared during authentication;
		(3)	the existence of a right to access identity information and the process for making requests for such access;
		(4)	the time and manner during which identity information will be stored;
		(5)	how the registered person may lodge a grievance or seek redress in relation to any improper use of the identity information; and
		(6)	the registered person's rights in accordance with section **Error! Reference source not found.**.

Information verification	**16.**	(a)	The MDIDS Administrator must verify the validity, authenticity and accuracy of identity information collected in the registration process by comparing such information with identity information recorded in the national identity card registration system, the work permit registration system and the visa registration system, as applicable.
		(b)	The verification process undertaken in accordance with subsection (a) seeks for the MDIDS Administrator to attain a high degree of certainty that:
		(1)	no person is registered more than once in the Maldives Digital Identity System;
		(2)	no person has more than one (1) Maldives Digital Identity Number and associated token;
		(3)	no Maldives Digital Identity Number or associated token is assigned to more than one (1) person; and
		(4)	no Maldives Digital Identity Number or associated token is assigned to a non-eligible person.
		(c)	After verifying the identity information obtained in accordance with this section, the MDIDS Administrator must:
		(1)	register the person as a registered person;
		(2)	record the prescribed biographic information and biometric information of the person in the MDIDS database; and
		(3)	assign to the person a Maldives Digital Identity Number and an associated token, as applicable, and inform the person of such Maldives Digital Identity Number and associated token.
		(d)	The limitations set forth in subsections (b)(1) and (b)(2) do not apply to protected persons that may be registered more than once or be assigned more than one (1) Maldives Digital Identity Number or associated token in accordance with regulations that may be made by the Maldives Police Service, or its successor, from time to time.

Inclusion and accessibility measures	**17.**	(a)	To promote inclusion and participation in the Maldives Digital Identity System, the MDIDS Administrator:
		(1)	must adopt special measures to facilitate registration of vulnerable groups including women, minors, senior citizens, persons with disabilities, and such other categories of persons as may be specified by regulations;
		(2)	may, directly or through third parties, establish physical establishments at suitable locations to facilitate registration of eligible persons in the manner established under regulation; and
		(3)	must comply with internationally accepted standards for accessibility when designing web and mobile applications for purpose of registration and implementation of the Maldives Digital Identity System.
		(b)	Notwithstanding the requirements set forth in section 15(b)(2), the MDIDS Administrator must make regulations establishing:
		(1)	special procedures and alternative types of biometric information to be collected from eligible persons that, for justified reasons, are unable to provide the biometric information established in this Act; and
		(2)	the option to grant a registered person a waiver from biometric information collection requirements set forth in this Act under exceptional circumstances and subject to specific approval by the MDIDS Administrator.

CHAPTER 5 **DITIGAL IDENTITY**			
Maldives Digital Identity Numbers and tokens	**18.**	(a)	Upon registration of an eligible person in accordance with **Error! Reference source not found.**Chapter 4, the MDIDS Administrator must assign to that registered person a Maldives Digital Identity Number and notify such person of the assigned Maldives Digital Identity Number through such means as prescribed by regulation.
		(b)	In addition to the assignment of a Maldives Digital Identity Number in accordance with subsection (a), the MDIDS Administrator may issue a token associated with that Maldives Digital Identity Number for use in place of such Maldives Digital Identity Number to strengthen protection and security of information and the integrity and reliability of the Maldives Digital Identity System.
		(c)	A Maldives Digital Identity Number and any associated token:
		(1)	must be a globally unique number assigned to a registered person solely for the purpose of identification or authentication in accordance with the Act;
		(2)	must be generated using a method established by regulation that ensures:
		(i)	unpredictability, meaning that the Maldives Digital Identity Number or associated token cannot be guessed or derived using any known identity information about the registered person;
		(ii)	non-linkability, meaning that the Maldives Digital Identity Number or associated token must not reveal, encode, or be mathematically derivable from identity information of the registered person to whom it is assigned; and

		(iii)	persistence of uniqueness, meaning that the Maldives Digital Identity Number or associated token must not be reused or reassigned, and it must remain unique across all registered persons and entities within the Maldives Digital Identity System; and
		(3)	may include one or more digits or characters calculated using a cryptographic or integrity-checking function as prescribed in regulation, provided such functions do not compromise the requirements set forth in subsection (2).
		(d)	No portion of the Maldives Digital Identity Number and any associated token, whether in full or in part, may be used to infer, derive, or imply any biometric information or demographic information of the registered person to whom it is assigned.
		(e)	A Maldives Digital Identity Number and any associated token must not carry or be associated with metadata or internal system codes that could be used to re-identify the individual without access to controlled reference data.
		(f)	A Maldives Digital Identity Number or associated token assigned to a registered person may not be assigned to another person, even after the registered person is deceased or the number has been deactivated.
		(g)	Subject to section 19, a registered person must have the same Maldives Digital Identity Number for the duration of his or her life.
Deactivation of Maldives Digital Identity Numbers and tokens	**19.**	(a)	The MDIDS Administrator must deactivate a registered person's Maldives Digital Identity Number:
		(1)	within 30 days after:
		(i)	the registered person's death is recorded in the national identity card registration system; or

		(ii)	the registered person ceases to hold a work permit or other resident visa allowing him or her to lawfully reside in the Maldives, provided such person has not become a citizen or is not eligible to renew such permit or visa; or
		(2)	promptly if the MDIDS Administrator reasonably believes that the integrity and reliability of the Maldives Digital Identity System has been or may likely be compromised in relation to that Maldives Digital Identity Number as a result of the manner of its issuance, a data breach or other breach of data security.
		(b)	The MDIDS Administrator must deactivate a token:
		(1)	immediately if the associated Maldives Digital Identity Number has been deactivated;
		(2)	promptly if the MDIDS Administrator reasonably believes that the integrity and reliability of the Maldives Digital Identity System has been or may likely be compromised in relation to that token as a result of the manner of its issuance, a data breach or other breach of data security; or
		(3)	at such time as the MDIDS Administrator considers convenient for the management of the Maldives Digital Identity System considering the use by relying parties of the token in identifying that registered person.
		(c)	Upon deactivation in accordance with this section, the MDIDS Administrator must:
		(1)	promptly inform the identity information providers of the deactivation of a Maldives Digital Identity Number or associated token; and
		(2)	notify any relevant relying parties of the deactivation of a Maldives Digital Identity Number or associated token.
		(d)	The MDIDS Administrator must make regulations establishing procedures and requirements for deactivation of Maldives Digital Identity Numbers and associated tokens under this Act.

Authenticators	**20.**	(a)	The following authenticators may be created under the Maldives Digital Identity System:
		(1)	a symbol provided by the MDIDS Administrator that encodes such identity information provided for under this Act and its regulation in a manner that is readable by an electronic device; or
		(2)	an application offered by the MDIDS Administrator to be installed on a personal communications device that contains such identity information as may be determined by the MDIDS Administrator and that is readable by an electronic device; or
		(3)	a digitally enabled physical identity card issued by the Department of National Registration that displays identity information provided in manner consistent with this Act and regulations made by the Minister under it.
		(b)	The MDIDS Administrator must issue authenticators to a registered person upon registration, provided that the number of authenticators that may be issued to the same registered person may be limited by regulation.
		(c)	The MDIDS Administrator must determine, and may modify from time to time, the specific type of authenticator and identity information that will be included in or associated with an authenticator issued in accordance with subsection (b).
		(d)	The Department of National Registration may issue digitally enabled physical identity cards in accordance with this Act in the manner and form prescribed by regulation issued by the Minister.
		(e)	Subject to the limitations established in subsection (f), the Department of National Registration must determine, and may modify from time to time, the specific core identity attributes that will be displayed in a digitally enabled physical identity card issued in accordance with subsection (d).

		(f)	In considering which core identity attributes may be included, stored or displayed on an authenticator assigned under this Act, the MDIDS Administrator and the Department of National Registration must weigh the utility of including, storing or displaying such attributes against the potential risks to the privacy and security of such identity information.
		(g)	As prescribed by regulations made by the Minister, a digitally enabled physical identity card may be readable by an electronic device and for that purpose may include an embedded microchip, QR code, bar code or other technology capable of recording the relevant identity information.
Obligations of registered persons	**21.**	A registered person must at all times:	
		(a)	Take appropriate measures to prevent another person accessing or using an authenticator stored in a personal communications device, except as permitted under this Act or its regulations;
		(b)	Safeguard and preserve in good form a digitally enabled physical identity card issued to him or her; and
		(c)	Promptly notify the MDIDS Administrator or the Department of National Registration, as applicable, if the registered person has reasonable grounds to believe that:
		(1)	another person has accessed his or her authenticator without permission or whether such authenticator has been tampered with; or
		(2)	the digitally enabled physical identity card issued to him or her has been lost, stolen, damaged or destroyed.
Responsibility and authority of parents and legal guardians	**22.**	(a)	The parents or the legal guardian of a minor have the authority to access the Maldives Digital Identity Number, associated token or authenticator issued to their dependent minor.

		(b)	The parents, jointly and severally, or the legal guardian of a minor are responsible for the use of the Maldives Digital Identity Number, associated token or authenticator issued to their dependent minor.
		(c)	In the absence of evidence to the contrary, the parents or the legal guardian of a minor are liable for any misuse of, or any offense committed against this Act or any other law using the Maldives Digital Identity Number, associated token or authenticator issued to their dependent minor.
		(d)	The parents or the legal guardian are authorized to consent to authentication requests from relying parties on behalf of their dependent minor.
Granting authorization to another person	**23.**	(a)	Subject to subsection **Error! Reference source not found.** (c), a registered person (first person) may digitally authorize via the Maldives Digital Identity System another registered person (second person) to access the first person's Maldives Digital Identity Number, associated token or an authenticator to authenticate the first person's identity in accordance with this Act.
		(b)	In the absence of evidence to the contrary, the second person is liable for any misuse of, or any offense committed against this Act or any other law using, the Maldives Digital Identity Number, associated token or authenticator of the first person.
		(c)	The provisions of subsection (a) do not apply to transactions where any applicable law requires an executed power of attorney or other legal instrument to be submitted to the grant of such authorization.
Cancellation of authenticators	**24.**	(a)	The MDIDS Administrator or the Department of National Registration, as applicable, must cancel an authenticator issued under this Act in accordance with subsection (b).
		(b)	An authenticator must be canceled under any of the following circumstances:

		(1)	the registered person's Maldives Digital Identity Number, or an associated token on or in the authenticator, is deactivated;
		(2)	duplicative digitally enabled physical cards have been issued in relation to the same registered person, except as authorized by law or regulation;
		(3)	there is reason to believe that the authenticator, or the device that stored it, was lost, stolen, damaged or destroyed, or has been obtained or accessed without permission or tampered with; or
		(4)	there is reason to believe that the authenticator was issued relying on false information or is likely to be used in a manner that undermines the integrity and/or reliability of the Maldives Digital Identity System.
		(c)	Upon cancellation of an authenticator, the MDIDS Administrator or the Department of National Registration, as applicable, must notify:
		(1)	the affected registered person of the cancellation of his or her authenticator; and
		(2)	relying parties seeking to use the authentication function in relation to a cancelled authenticator.
		(d)	The Maldives Digital Identity System will no longer perform authentication functions for a registered person relying on the cancelled authenticator.
		(e)	Notwithstanding the generality of subsection **Error! Reference source not found.**(d), in the event that a cancellation is made pursuant to subsection (b)(3) the MDIDS Administrator or Department of National Registration may reissue an authenticator to the registered person as prescribed by regulations.

CHAPTER 6 **AUTHENTICATION FUNCITON**			
Authentication function	**25.**	The MDIDS Administrator must:	
		(a)	perform authentication of a registered person's identity within the Maldives Digital Identity System;
		(b)	establish procedures, protocols and standards for authentication to be implemented in the Maldives Digital Identity System and used by relying parties;
		(c)	offer different modes of authentication with a view of technology and security developments as prescribed by regulation; and
		(d)	allow for different identity assurance levels as prescribed by regulation.
Use of the authentication function	**26.**	(a)	Relying parties may request the use of the authentication function of the Maldives Digital Identity System in accordance with this Act and the technical requirements and procedures prescribed by regulation.
		(b)	At the time of authentication, a relying party must inform the registered person of the following:
		(1)	the identity information that will be shared by the MDIDS Administrator upon authentication;
		(2)	the uses to which the identity information received during authentication may be put; and
		(3)	such alternative means of authentication that are available to the registered person.
		(c)	After communicating the information in accordance with subsection (b), a relying party must, in the manner and form as may be specified by the MDIDS Administrator in regulation:
		(1)	obtain consent from the registered person to proceed with the authentication; and

		(2)	maintain logs or records of the consent obtained.
		(d)	Relying parties must comply with procedures and requirements for authentication of registered persons and obtaining information from the MDIDS database as may be prescribed by regulation.
		(e)	Relying parties must provide alternative means for a person to prove his or her identity, if such persons is:
		(1)	not a registered person;
		(2)	unable to produce a Maldives Digital Identity Number, associated token, or authenticator; or
		(3)	unable to be authenticated by the Maldives Digital Identity System.
Collection of data for authentication	**27.**	(a)	The MDIDS Administrator must determine:
		(1)	the identity information that a relying party must collect, transmit and process for the Maldives Digital Identity System to authenticate a registered person;
		(2)	applicable security and privacy safeguards consistent with internationally acceptable standards that a relying party must comply with when collecting, transmitting and processing identity information for purposes of authentication; and
		(3)	the manner of such collection, transmission and processing of identity information.
		(b)	Collection, transmission and processing of identity information in accordance with subsection (a) must be limited to the minimal set of data that the relying party requires to provide its services.
Authentication transaction data records	**28.**	(a)	The MDIDS Administrator must store authentication function records including:
		(1)	authentication requests and transactions;
		(2)	metadata, including date stamps, search logs and audit trails; and
		(3)	such other records as may be determined by the MDIDS Administrator.

		(b)	Authentication transaction data records must be retained by the MDIDS Administrator for a period of five (5) years.
		(c)	Notwithstanding the generality of subsection (a), the Maldives Digital Identity System may under no circumstances store data on the purpose of authentication.
		(d)	Authentication transaction data records may be used, and must be accepted by courts or other agencies, to provide sufficient legal proof that a relying party has authenticated a registered person's identity through the Maldives Digital Identity System when such relying party is required by law or regulation to identify or authenticate a person.
		(e)	Upon expiry of the storage period specified in subsection (b), authentication transaction data records must be deleted except when such records are required to be maintained by a court or in connection with any pending dispute.
Relying parties must retain transaction data records	**29.**	(a)	A relying party must retain records of authentication transactions such relying party has processed in the manner and for such duration as may be determined by the MDIDS Administrator.
		(b)	Records retained in accordance with subsection (a) may not include identity information of a registered person, but may include:
		(1)	the Maldives Digital Identity Number for which authentication was requested;
		(2)	information on the authentication request submitted;
		(3)	information received as authentication response;
		(4)	the record of disclosure of information to the registered person at the time of authentication;
		(5)	the record of consent of the registered person to undertake the authentication; and

		(6)	the record and authorizations for transactions undertaken in accordance with sections 22 and 23**Error! Reference source not found.**.
		(c)	A relying party must not share the authentication records retained in accordance with this section with any person other than:
		(1)	the affected registered person upon their request or for grievance redressal and resolution of disputes; or
		(2)	with the MDIDS Administrator for audit purposes; or
		(3)	such other public agency as may be authorized by law, regulation or court order to have access to such records.
		(d)	A relying party must comply with all relevant laws, rules and regulations, including, but not limited to, [REFERENCE TO DIGITAL LEGISLATIVE PACKAGE TO BE INCLUDED], in relation to the retention of records under this section.
		(e)	The obligations relating to authentication records as specified in this section will apply even if a relying party's participation in the Maldives Digital Identity System is canceled or suspended in accordance with section 10(f)(4).
Access to authentication records by registered persons	**30.**	A registered person has the right to access their authentication records subject to the procedures, requirements and conditions laid down in regulation and the payment of such fees, as may be prescribed by the MDIDS Administrator by regulation.	
CHAPTER 7 **PRIVACY PROTECTIONS**			
Application of the Personal Data Protection Act		(a)	The obligations and principles set forth in the Personal Data Protection Act will apply, without exception, to following agencies, entities and persons in relation to the actions, functions and responsibilities undertaken in accordance with this Act:

		(1)	the MDIDS Administrator;
		(2)	the identity information providers;
		(3)	relying parties; and
		(4)	data processors.
		(b)	Without limiting subsection (a), the MDIDS Administrator, identity information providers, relying parties and data processors, must ensure that identity information is:
		(1)	collected only to the extent and for the purposes specified in this Act and regulations made under it and not further processed in a manner inconsistent with those purposes;
		(2)	adequate, relevant and limited to the minimum necessary for the purposes for which the identity information was collected or further processed;
		(3)	retained for the period established in this Act or regulations made under it; and
		(4)	accurate, complete and current as prescribed in this Act.
Prohibition of processing certain special categories of personal data	**31.**	(a)	With the exception of biometric information that is collected, stored, used or disclosed exclusively for the purpose of the registration or authentication functions established in the Act, the MDIDS Administrator, relying parties and data processors must not collect, store, use or disclose any other special categories of personal data as defined in the Personal Data Protection Act for purpose of implementing this Act.
		(b)	The MDIDS Administrator, relying parties and data processors may only disclose biometric information collected under this Act:
		(1)	to a law enforcement agency in accordance with a warrant or other valid court order;
		(2)	to the registered person to whom the biometric information relates; or
		(3)	for purpose of undertaking testing in relation to the biometric information in compliance with any purposes, processes, ethics obligations and requirements set forth by regulation;

		(c)	The MDIDS Administrator may make regulations in relation to the collection, use, disclosure, storage or destruction of biometric information in accordance with this Act in manner that protects the privacy and security of such information and is consistent with generally accepted international standards.
Identity information must not be used or disclosed	**32.**	The MDIDS Administrator, relying parties and data processors must not use or disclose identity information about a registered person that is in their possession or under their control for any of the following purposes:	
		(a)	offering to supply goods or services;
		(b)	advertising or promoting goods or services;
		(c)	enabling another entity to offer to supply goods or services;
		(d)	enabling another entity to advertise or promote goods or services;
		(e)	market research; or
		(f)	any other commercial purposes.
Data breach notifications	**33.**	(a)	The MDIDS Administrator, relying parties and data processors must notify data breaches affecting identity information in their possession or control pursuant to this Act in the manner and form established in the Personal Data Protection Act.
		(b)	Relying parties and data processors must give a copy of the notification submitted in accordance with subsection (a) to the MDIDS Administrator at the same time as such notice is given to the Data Protection Authority.

CHAPTER 8 **SECURITY MEASURES**			
Security, integrity, and confidentiality	**34.**	(a)	The MDIDS Administrator, the identity information providers, relying parties and data processors acting on their behalf must implement appropriate technical and organizational measures that are compliant with generally accepted international standards to ensure the security, integrity and confidentiality of identity information in their possession or under their control in connection with this Act.
		(b)	Measures adopted in accordance with subsection (a) must include, but are not limited to, safeguards against accidental or unlawful destruction, loss, misuse or alteration, unauthorized disclosure or access to identity information.
		(c)	The determination of appropriate measures required in accordance with subsection (a), must take account of the following factors:
		(1)	the quantity and sensitive nature of identity information;
		(2)	the likelihood of risks and harms to registered persons from the loss, disclosure or other misuse of their identity information;
		(3)	the extent of the processing of identity information undertaken or expected to be undertaken; and
		(4)	the cost of implementing specific measures, including technologies, systems and tools needed, relative to the resources available to the specific public agency, entity or person.
		(d)	Regulations made under this Act may establish specific measures, requirements and conditions to implement this section.

CHAPTER 9 **DIGITAL WALLET**			
Approval and use of a digital wallet	**35.**	(a)	The MDIDS Administrator may approve and support the use of a digital wallet for the storage and presentation of verifiable credentials and other identity information, in accordance with regulations made under this Act.
		(b)	The MDIDS Administrator must ensure that any digital wallet approved under this Act:
		(1)	complies with applicable international interoperability and security standards for verifiable credentials and digital identity wallets, as prescribed by regulation;
		(2)	supports consent-based disclosure, whereby a registered person can selectively share only those identity attributes required for a given transaction;
		(3)	includes mechanisms for revocation, suspension, or expiration of verifiable credentials where required; and
		(4)	provides the registered person with transparency and auditability features allowing the review of usage and sharing history of verifiable credentials.
The MDIDS Administrator may issue or authorize issuance of verifiable credentials	**36.**	(a)	The MDIDS Administrator may issue or authorize third parties to issue verifiable credentials that are cryptographically signed, portable, and compatible with the digital wallet, provided such issuance complies with the governance and technical standards under this Act and its regulations.
		(b)	A digital wallet may contain the following types of verifiable credentials or identity information, subject to the regulations and the consent of the registered person:
		(1)	core identity attributes registered under the Maldives Digital Identity System;

		(2)	additional verifiable credentials issued by public agencies, legal entities, or other approved issuers; and
		(3)	authentication tokens or keys linked to authenticators established under this Act.
Conditions and requirements for digital wallets	**37.**	(a)	The MDIDS Administrator may prescribe by regulation:
		(1)	the functional, technical, and interoperability requirements for digital wallets;
		(2)	conditions under which digital wallets may be used in online or in-person authentication;
		(3)	requirements for the protection of private keys and prevention of unauthorized access or tampering;
		(4)	the criteria for recognition or accreditation of digital wallet providers or verifiable credential issuers; and
		(5)	the process for updating or migrating credentials, including those affected by name changes, expiry, or fraud.
		(b)	The MDIDS Administrator must consider the protection of the privacy, autonomy, and security of registered persons in all decisions relating to digital wallets and verifiable credentials, including in the approval of formats, issuance methods, and standards.
Voluntary nature	**38.**	For avoidance of doubt, nothing in this chapter may be interpreted to mandate the use of a digital wallet or verifiable credentials, the use of which is voluntary and must not preclude the use of alternative authenticators as provided for under this Act.	

CHAPTER 10 FEES			
Charging fees by the MDIDS Administrator	**39.**	(a)	Regulations made under this Act may allow the MDIDS Administrator to charge fees for activities carried out, directly or through another party, to perform the functions and responsibilities set forth in this Act and its regulations.
		(b)	The regulations made in accordance with subsection (a) may provide for the following:
		(1)	determine the amount of fees or the method of calculating the fees;
		(2)	determine that a fee may allow recovery of the cost incurred by the MDIDS Administrator in arranging and paying another party to carry out a relevant activity;
		(3)	establish the time and manner in which fees must be paid;
		(4)	set forth penalties for late payment of specified fees; and
		(5)	provide for the refund, reduction or waiver of specified fees or penalties for late payment of specified fees.
		(c)	The regulations made in accordance with subsection (a) must not establish a fee to be charged to an eligible person:
		(1)	for registration with the Maldives Digital Identity System; or
		(2)	for the assignment of a Maldives Digital Identity Number or associated token or authenticator; or
		(3)	for the initial issuance of digitally enabled physical identity card.
		(d)	The fees or revenue collected by the MDIDS Administrator will be credited to the consolidated revenue fund.

		(e)	A fee charged by the MDIDS Administrator that is due and payable under this Act as well as associated penalties for late payment of specified fees may be recovered as a debt by action in a court of competent jurisdiction.
CHAPTER 11 **GRIEVANCE REDRESS MECHANISMS**			
Grievances redress mechanisms	**40.**	(a)	A registered person may lodge queries and grievances with the MDIDS Administrator in relation to conduct deemed contrary to the obligations and protections set forth in this Act and obtain timely and effective resolution of such queries and grievance.
		(b)	The MDIDS Administrator must establish accessible and secure procedures for lodging and resolving queries and grievance as prescribed in regulation.
CHAPTER 12 **ADMINISTRATION**			
Consequential amendments to the Penal Code	**41.**	(a)	The Penal Code is amended as follows:
		(1)	in section 312(b) insert "including a digital form of identification or a digital authenticator or verifiable credential." after "used to identify the person".
		(2)	by adding a new section [TBD] which reads as follows: "**Section [TBD] – Impersonation to register in the Maldives Digital Identity System** (a) Offense Defined. A person commits an offense if:

			(1) he registers falsely in the Maldives Digital Identity System as another person, whether the latter is alive or dead, (2) by submission of false biographical information or biometric information, (3) or attempts to do so. (b) Definition. The Maldives Digital Identity System, biographical information and biometric information have the meaning established in the Digital Identity Act. (c) Grading. The Offense is a Class 1 misdemeanor.
		(3)	by adding a new section [TBD] which reads as follows: "**Section [TBD] – Unlawful collection of identity information** (a) Offense Defined. A person commits an offense if: (1) not being authorized to collect identity information under the provisions of the Digital Identity Act, (2) by words, conduct or demeanor, (3) knowingly pretends that he is authorized to do so. (b) Definition. Identity information has the meaning established in the Digital Identity Act. (c) Grading. The Offense is a Class 1 misdemeanor.
		(4)	by adding a new section [TBD] which reads as follows: "**Section [TBD] – Unlawful disclosure of identity information** (a) Offense Defined. A person commits an offense if: (1) without lawful excuse or authority,

			(2) discloses, transmits, copies or otherwise disseminates, (3) any identity information collected or otherwise processed in the course of registration or authentication with the Maldives Digital Identity System or through a digital wallet, (4) to any person not authorized under the Digital Identity Act or regulations made under the Digital Identity Act. (b) Definition. The Maldives Digital Identity System, identity information, registration, authentication and digital wallet have the meaning established in the Digital Identity Act. (c) Grading. The Offense is a Class 1 misdemeanor.
Non-compliance by relying parties and data processors or authorized provider of verifiable credentials	**42.**	(a)	A relying party, a data processor or an authorized provider of verifiable credentials who fails to comply with any provision of this Act or regulations made under it is liable to civil penalties in the form of a fine:
		(1)	not exceeding MVR 50,000 for the first failure to comply; and
		(2)	not exceeding MVR 100,000 for any subsequent failures to comply with the same obligation.
		(b)	The MDIDS Administrator may, at any time, require relying parties and data processors and authorized providers of verifiable credentials to provide any reasonable information relating to their activities under this Act to verify their compliance with the Act.

CHAPTER 13 TRANSITION PROVISIONS			
Preexisting relying parties and data processors	**43.**	(a)	Any relying party or data processor appointed prior to the commencement of this Act for purpose of implementing digital identity in the Republic of the Maldives in accordance with the eFaas service will be deemed to continue in such roles and all agreements entered into by such entities and the National Center for Information Technologies or other public agencies will continue to be in force to the extent not inconsistent with the provisions of this Act, its regulations or the policies, processes, procedures, standards and specifications issued by the MDIDS Administrator.
		(b)	Notwithstanding the generality of subsection (a), within twelve (12) months from the date this Act comes into force, any preexisting relying party:
		(1)	must comply with:
		(i)	the provisions of this Act and regulations made under it, and
		(ii)	the policies, processes, procedures, standards and specifications issued by the MDIDS Administrator; and
		(2)	may be required to amend existing agreements or enter into such other agreements in the manner and timeframe as the MDIDS Administrator may determine.

		(c)	In the event any such public agency, entity or person referred to subsection (a) intends to discontinue using the authentication function as specified in this Act, it must make an application for termination to the MDIDS Administrator and comply with any discontinuation requirements as may be specified by the MDIDS Administrator by regulation.
Transition of the eFaas database	**44.**	(a)	The eFaas digital identity service and database developed and managed by or on behalf of the National Center for Information Technologies will continue to operate and must be transitioned into the MDIDS database described in section **Error! Reference source not found.** 12 within a period of 6 (six) months from the date this Act comes into force.
		(b)	To undertake the transition processes established under subsection (a), the National Center for Information Technologies or the MDIDS Administrator, as applicable, must make such updates, upgrades or enhancements to ensure that the resulting MDIDS database is compliant with the requirements set forth in this Act and its regulations.
Transition to unique identity numbers and Maldives Digital Identity Numbers	**45.**	(a)	Identity information providers must transition existing sequential identity numbers assigned in accordance with the practices and methods in place prior to the entry into force of this Act to a national identity numbering system able to generate unique identity numbers for citizens and residents as established in this Act and its regulations.
		(b)	To achieve the objective set forth in subsection (a), within twelve (12) months from the date this Act comes into force identity information providers:
		(1)	may continue issuing sequential national identity card numbers, work permit numbers and visa numbers, as applicable, in accordance with the practices and methods in place prior to the entry into force of this Act;

		(2)	must establish capabilities and begin to generate unique identity numbers in a manner to ensure consistency with the method and requirements established for Maldives Digital Identity Numbers in accordance with this Act and its regulations; and
		(3)	must implement processes, timelines, conditions and requirements to convert previously assigned sequential identity numbers assigned to citizens and residents, as applicable, to unique identity numbers as provided in subsection (a).
		(c)	The Minister must make regulations to establish processes, timelines, conditions and requirements to implement the transition process provided in this section.
		(d)	Within three (3) months from the date this Act comes into force, the MDIDS Administrator and the identity information providers must establish coordination mechanisms to ensure effective implementation of this section.
CHAPTER 14 **MISCELLANEOUS**			
Making and implementation of regulations	**46.**	(a)	Unless otherwise provided in this Act, all regulations to be made pursuant to this Act must be made and implemented by the MDIDS Administrator.
		(b)	Regulations required to implement this Act must be made and published in the Government Gazette within a period of 6 (six) months from the date this Act comes into force.
		(c)	Within the period established in subsection (b), the MDIDS Adminstrator must make, at a minimum, the following regulations:
		(1)	Digital Identity (Registration) Regulations;
		(2)	Digital Identity (Authentication and Data Sharing) Regulations;
		(3)	Digital Identity (Security) Regulations; and

		(4)	Digital Identity (Fee) Regulations.
Commencement of Act	**47.**	This Act will come into force when it is passed, ratified and from the date it is published in the Government Gazette.	
Interpretation	**48.**	Unless the use of a word or phrase in this Act implies a different meaning, the following words and phrases have been given the meaning as specified below:	
		(a)	"authentication" refers to the process by which the Maldives Digital Identity System confirms the identity of a registered person to a relying party;
		(b)	"authenticator" means a device, application, credential, or other technology used to authenticate a registered person's identity in accordance with this Act;
		(c)	"attribute" of a person means information that is associated with that person and includes biographic and biometric information;
		(d)	"biographic information" means attributes of a person or their life that are not biometric information and include those specified in section 15(b)(1);
		(e)	"biometric information" means information about any measurable biological characteristic relating to a person that can be used to identify the person or verify the person's identity, and include biometric templates;
		(f)	"citizen" has the meaning established in Article 9 of the Constitution of the Republic of the Maldives;
		(g)	"consent" means any freely given, specific, informed, and unambiguous indication of an eligible person or a registered person's wishes by which they, through a statement or a clear affirmative action, signify agreement to the processing of identity information relating to them under this Act. Consent may be provided by a lawful representative or agent with the authority to act on behalf of an eligible person or a registered person;
		(h)	"data breach" has the meaning established in the Personal Data Protection Act;

		(i)	"data processor" means a person, legal entity, public agency who or which processes identity information on behalf of the MDIDS Administrator, an identity information provider or a relying party;
		(j)	"Department of National Registration" means the agency responsible for administration and management of the identity card registration system under the Act on Registration of Births and Deaths and Issuance of Birth Certificates and National Identity Cards (Law No. 23/2022);
		(k)	"digital identity" is a structured collection of electronically captured and stored attributes and authenticators that uniquely identify a person within a specific digital context. Digital identities enable individuals to authenticate themselves and access digital goods and services securely.
		(l)	"digital wallet" means an application or system that:
		(1)	resides on a personal communications device or other approved medium;
		(2)	is capable of securely storing, managing, and selectively disclosing identity attributes, verifiable credentials, or authentication tokens for the purpose of identification or authentication; and
		(3)	allows a registered person to prove hir or her identity or attributes in a manner that is privacy-preserving, cryptographically verifiable, and consistent with the technical and security standards prescribed by regulation.
		(m)	"eligible person" means a natural person that is:
		(1)	a citizen that has been issued a national identity card; or
		(2)	a resident holding a work permit; or
		(3)	a resident holding any other type of visa not covered in subsection (2) that allows that person to legally reside in the Maldives.

		(n)	"foundational identity databases" means the national databases identified in this Act that are single source of truth for eligible person's identity information.
		(o)	"identity information" means biographic information and biometric information and any other information relating to a person who can be identified or is identifiable, directly or indirectly by reference to such information;
		(p)	"legal guardian" means a person to whom the legal responsibility of a minor has been entrusted by a judgment of the competent court of law;
		(q)	"Maldives Digital Identity Number" means a unique number issued by the MDIDS Administrator to each registered person in accordance with section 18;
		(r)	"Maldives Digital Identity System" or "MDIDS" has the meaning established under section **Error! Reference source not found.**5;
		(s)	"MDIDS Administrator" means the Maldives Digital Services, an independent agency created under the Maldives 2.0 Act, or its successor agency;
		(t)	"Minister" means the minister entrusted from time to time with the responsibility for the administration and oversight of digital services and information technologies in the Maldives;
		(u)	"minor" means a person below the age of 18 years.
		(v)	"national identity card registration system" means the national identity card electronic database established and maintained by the Department of National Registration pursuant to the Act on Registration of Births and Deaths and Issuance of Birth Certificates and National Identity Cards (Law No. 23/2022) and the associated systems for notification and registration, and its successor databases and evolutions, as applicable;
		(w)	"person" means natural person;
		(x)	"public agency" means:

		(1)	the Government of Maldives, including any Ministry, department, agency, or other institution or instrumentality;
		(2)	state owned entities; and
		(3)	any other statutory body;
		(y)	"registered person" means an eligible person that has registered with the Maldives Digital Identity System in accordance with Chapter 4;
		(z)	"registration" means the process by which the prescribed biographic and biometric information about an eligible person is verified and recorded in the MDIDS database;
		(aa)	"relying party" means any public agency, legal entity or a person that is approved as such by the MDIDS Administrator in accordance with this Act and is entitled to rely, or seek to rely, on the Maldives Digital Identity System for authentication of a registered person;
		(bb)	"representative" means a parent, legal guardian, or family member lawfully acting on behalf of an eligible person or a registered person;
		(cc)	"resident" means a person who is not a citizen and who is lawfully permitted to reside in the Maldives under a relevant law;
		(dd)	"revocation" means the process by which a verifiable credential, authenticator, or identity attribute is rendered invalid or no longer trustworthy, either temporarily or permanently, by the issuing authority or MDIDS Administrator in accordance with this Act or its regulations;
		(ee)	"token" means a unique number that is exclusively associated with a Maldives Digital Identity Number and that is issued by the MDIDS Administrator to a registered person in accordance with this Act;
		(ff)	"verifiable credential" means a tamper-evident credential with authorship that can be cryptographically verified;

		(gg)	"visa registration system" means the electronic database that contains identity information on visa holders that do not hold work permits established by the competent public agency and the associated systems for notification and registration, and its successor databases and evolutions, as applicable;
		(hh)	"work permit registration system" means the work permit electronic database established and maintained by the public agency entrusted from time to time with the responsibility to develop and maintain work permits for certain residents and the associated systems for notification and registration, and its successor databases and evolutions, as applicable.