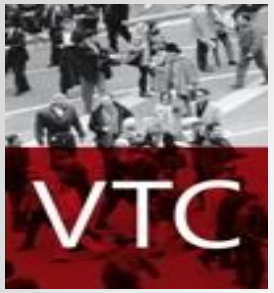


Clouddiensten bij de overheid

DPO-studiedag 27 november 2023

Hans Graux en Erik Van Zuren

Cloudstrategie van de Vlaamse overheid – 7 februari 2019

In deze Vlaamse overheidsbrede cloudstrategie worden 6 strategische principes naar voor geschoven:

1. **We kiezen voor een publieke cloud-first strategie**

   Evalueer eerst cloud vooraleer andere alternatieven te beschouwen. Dit is in de praktijk geen 'cloud only' strategie.

2. **We voorzien een multi-cloud aanbod binnen de Vlaamse overheid**

   Zo kunnen entiteiten individueel telkens de meest effiënte en geoptimaliseerde keuze maken.

3. **Alle entiteiten maken een plan van aanpak die past in een cloud adoptie pad, om de cloudstrategie te concretiseren**

   Hierdoor kunnen entiteiten zich identificeren in een bepaalde fase en de hieraan gekoppelde acties als doel voorop stellen.

4. **We garanderen continuïteit via een hybride cloud architectuur**

   Dit zal gebruikt worden bij een cloud migratie.

5. **We werken risicobeheersmaatregelen uit op het niveau van de Vlaamse overheid**

   Dit om de informatieveiligheid te garanderen, de risico's in kaart te brengen en te mitigeren.

6. **We benutten maximaal de software- en platformdiensten van de cloud**

   Zo moeten geen eigen platformen en infrastructuur worden ingericht en onderhouden.

Dit houdt in dat standaard aanvragen voor IAAS/ PAAS diensten 'by default' beantwoord worden met diensten vanuit hyperscale public cloud.
De VO cloud strategie is geen 'cloud-only' strategie. Andere opties, zoals een "managed DC" of outsourced DC of ComputerZaal Faciliteiten (CZF) blijven ook mogelijk (na een gegronde evaluatie)

ICT-Raamcontracten, Cloud en datacenterdiensten

Resultaat? Sterke dominantie van AWS, Azure, O365, SAP, SalesForce, …

Europees? Een dans in twee richtingen…

PRO: innovatie, efficiëntie, security

- European Cloud Partnership
- GAIA-X
- Twee Europese AVG-gedragscodes
- Regulation on the free flow of non-personal data
- European cybersecurity certification scheme for cloud services (EUCS – Cybersecurity Act
- Data Privacy Framework

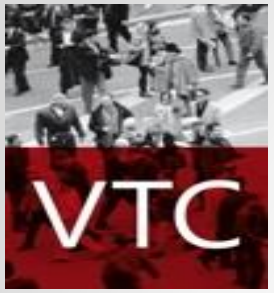
CONTRA: gegevensbescherming, autonomie, datasoevereiniteit

- Schrems
- EDPB - Coordinated Enforcement Action, use of cloud-based services by the public sector
- Data Act
- Digital Markets Act (gatekeepers)
- European Data Spaces
- (en bedenkingen bij de DPF…)

Beleidsmatige bezorgdheden

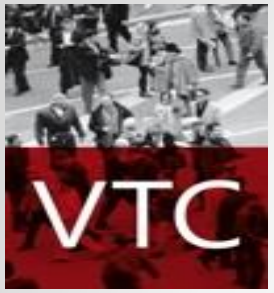
- Vanzelfsprekend toegang door/vanuit derde landen (Schrems)
- Veiligheidsopties zijn vaak zeer goed, maar worden ze gebruikt, en volstaan ze?
  - IaaS versus SaaS
- Gebruiksgemak leidt tot automatismen – wordt er nog grondig geëvalueerd?
- Het slot is degelijk, maar wie heeft de sleutels? Encryptie, beheersomgevingen, rights management
- Voorrang voor kost en gemak
- Lock-in, in meerdere vormen:
  - *“We moeten nu naar de cloud, we hebben geen andere keuze meer. Ons eigen datacenter bestaat niet meer / gaat volgende maand offline”*
  - *“We moeten nu naar deze cloud, want geen enkele concurrent voldoet”*
  - *“We kunnen nu niet meer uit deze cloud, dus we moeten deze wijzigingen slikken”*

Gegevensbescherming draait niet louter om privacy, maar ook om zorg voor de gegevens van de burger. Geen keuze meer? Dan is zorg ook niet meer mogelijk.

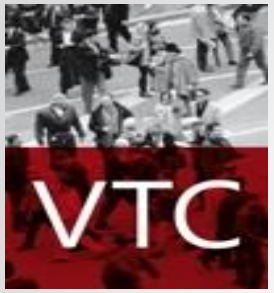


Dus anti-cloud?

- Nadrukkelijk niet.
- De ene cloud is de andere niet, en de VTC is niet blind voor de enorme potentiële voordelen
- Maar een cloud-automatisme is een risico, en ongepast vanuit het perspectief van gegevensbescherming
- Hoe beoordeel je dat?



Cloud?



NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-145

The NIST Definition of Cloud Computing

Recommendations of the National Institute of Standards and Technology

Peter Mell
Timothy Grance

Deployment Models:

Private cloud. The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud. The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

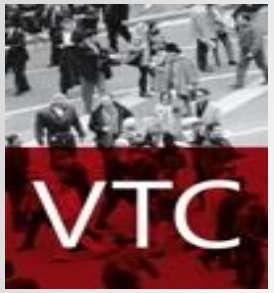
Hybrid cloud. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Service Models:

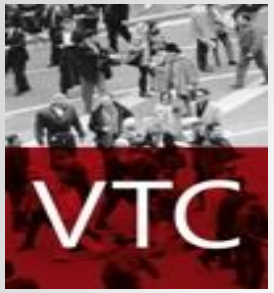
Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure[2]. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.[3] The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

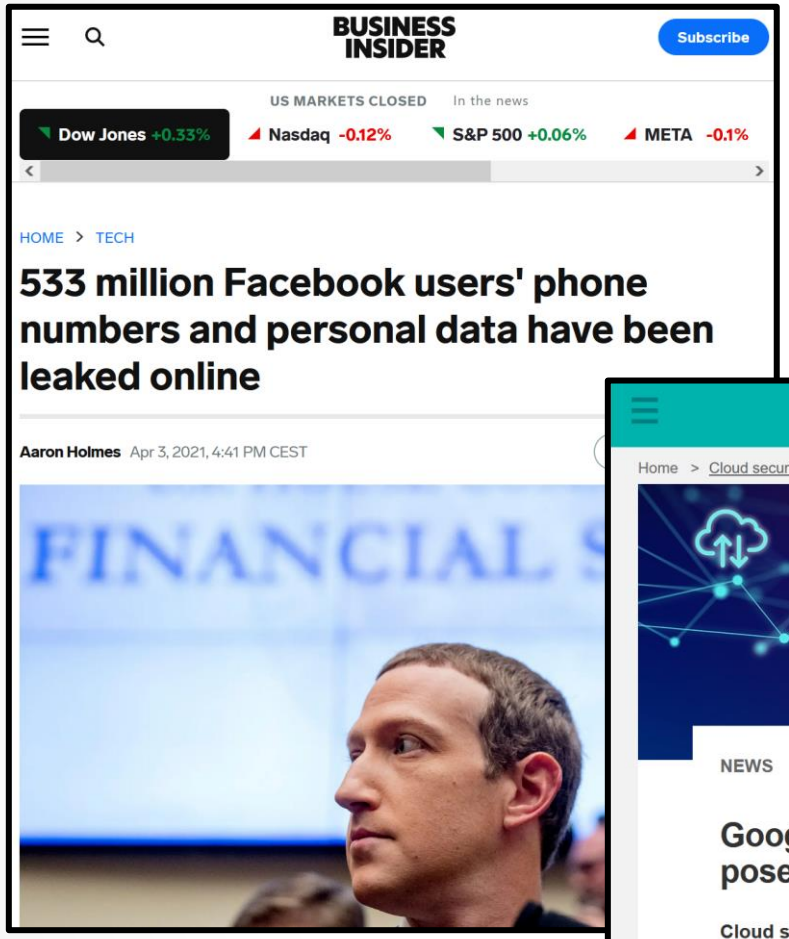
Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

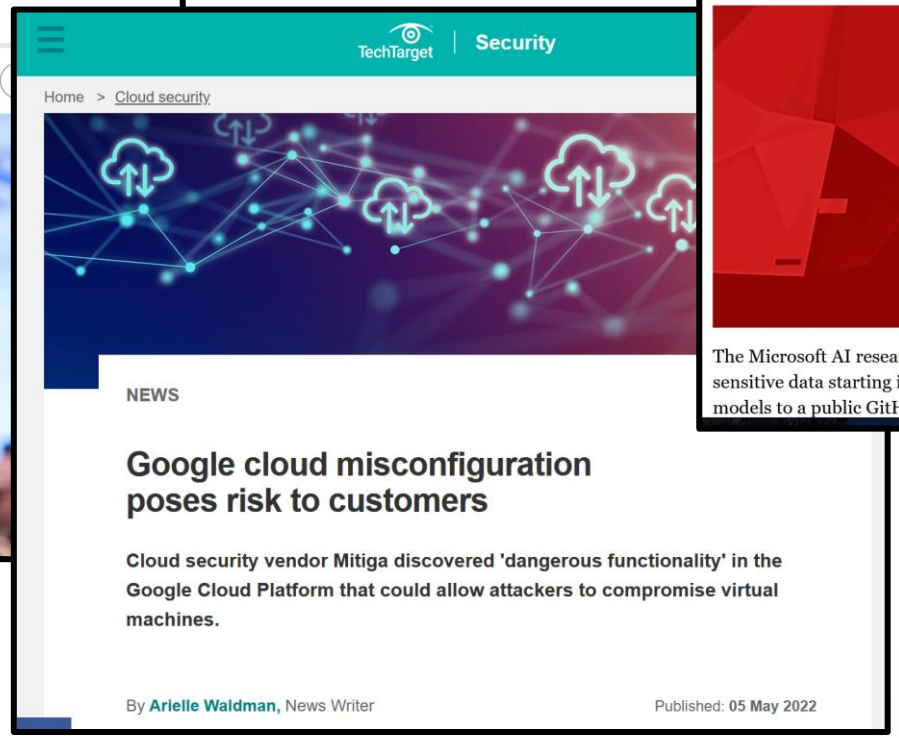


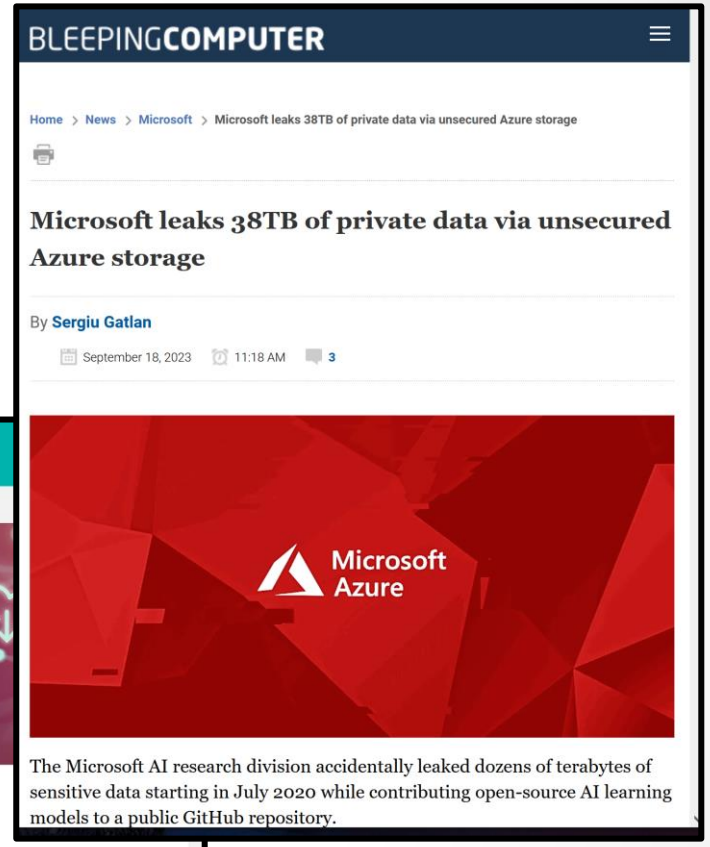
“ In het algemeen stelt de VTC vast dat nieuwe technische oplossingen duidelijke verbetering inhouden, maar….. “

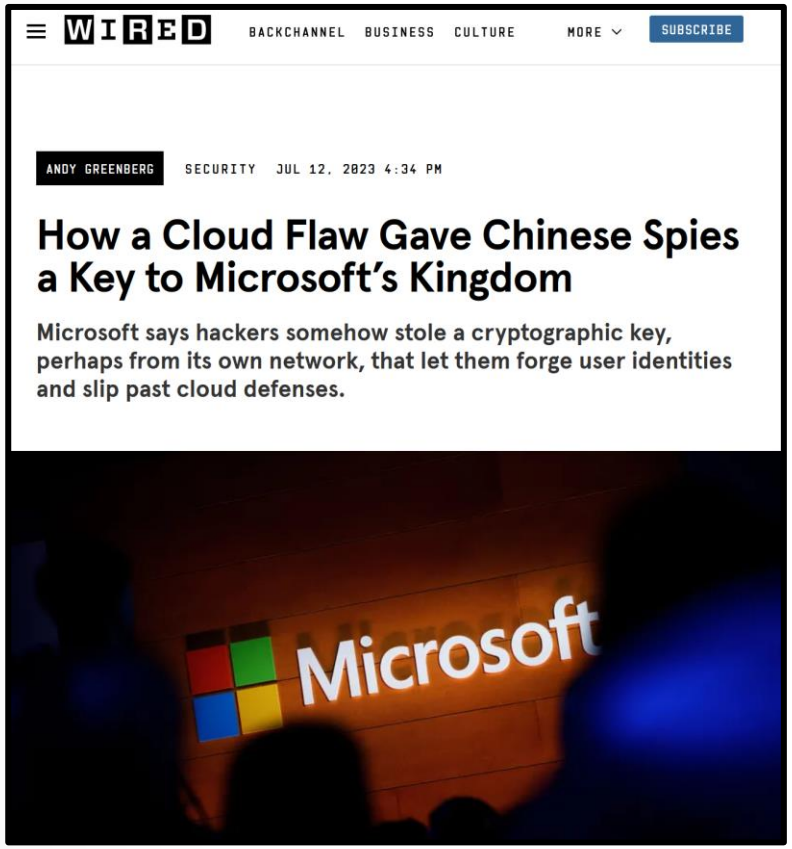


In Cloud we Trust?

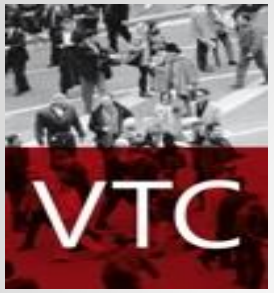

BUSINESS INSIDER
Subscribe
US MARKETS CLOSED
In the news
Dow Jones +0.33%
Nasdaq -0.12%
S&P 500 +0.06%
META -0.1%
HOME > TECH
533 million Facebook users' phone numbers and personal data have been leaked online
Aaron Holmes Apr 3, 2021, 4:41 PM CEST


TechTarget
Security
Home > Cloud security
NEWS
Google cloud misconfiguration poses risk to customers
Cloud security vendor Mitiga discovered 'dangerous functionality' in the Google Cloud Platform that could allow attackers to compromise virtual machines.
By Arielle Waldman, News Writer
Published: 05 May 2022


BLEEPINGCOMPUTER
Home > News > Microsoft > Microsoft leaks 38TB of private data via unsecured Azure storage
Microsoft leaks 38TB of private data via unsecured Azure storage
By Sergiu Gatlan
September 18, 2023
11:18 AM
3
Microsoft Azure
The Microsoft AI research division accidentally leaked dozens of terabytes of sensitive data starting in July 2020 while contributing open-source AI learning models to a public GitHub repository.


WIRED
BACKCHANNEL BUSINESS CULTURE MORE
SUBSCRIBE
ANDY GREENBERG
SECURITY JUL 12, 2023 4:34 PM
How a Cloud Flaw Gave Chinese Spies a Key to Microsoft's Kingdom
Microsoft says hackers somehow stole a cryptographic key, perhaps from its own network, that let them forge user identities and slip past cloud defenses.
Microsoft


BLEEPINGCOMPUTER
Home > News > Security > VMware fixes critical zero-day exploit chain used at Pwn2Own
VMware fixes critical zero-day exploit chain used at Pwn2Own
By Sergiu Gatlan
April 25, 2023 02:33 PM 0
vmware
VMware has released security updates to address zero-day vulnerabilities that could be chained to gain code execution systems running unpatched versions of the company's Workstation and Fusion software hypervisors.



Home / Security / News

UPDATED

Intel ‘Downfall’: Severe flaw in billions of CPUs leaks passwords and much more

There is a serious security flaw in billions of Intel CPUs that can let attackers steal confidential data like passwords and encryption keys. Firmware updates can fix it, but at a potential significant performance loss.

By Hans-Christian Dirscherl

Redakteur, PCWorld | AUG 12, 2023 7:00 AM PDT

The Record.
Recorded Future News

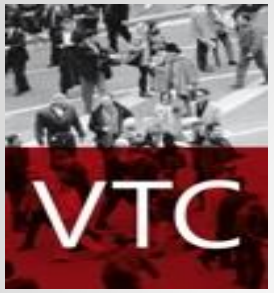
IMAGE: FLICKR / (STEPHAN) / CC BY-SA 2.0

Alexander Martin

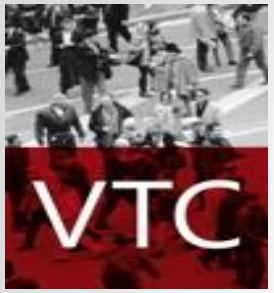
July 20th, 2023

North Korean hackers linked to attempted supply-chain attack on JumpCloud customers

North Korean hackers were behind a breach of the software business JumpCloud that formed part of an attempted supply-chain attack targeting cryptocurrency companies, it was reported on Thursday.



Hoe Data Protection zekerstellen?



REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 27 April 2016

on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

(78) The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processo
The principles of data protection by design and by default should also
tenders.

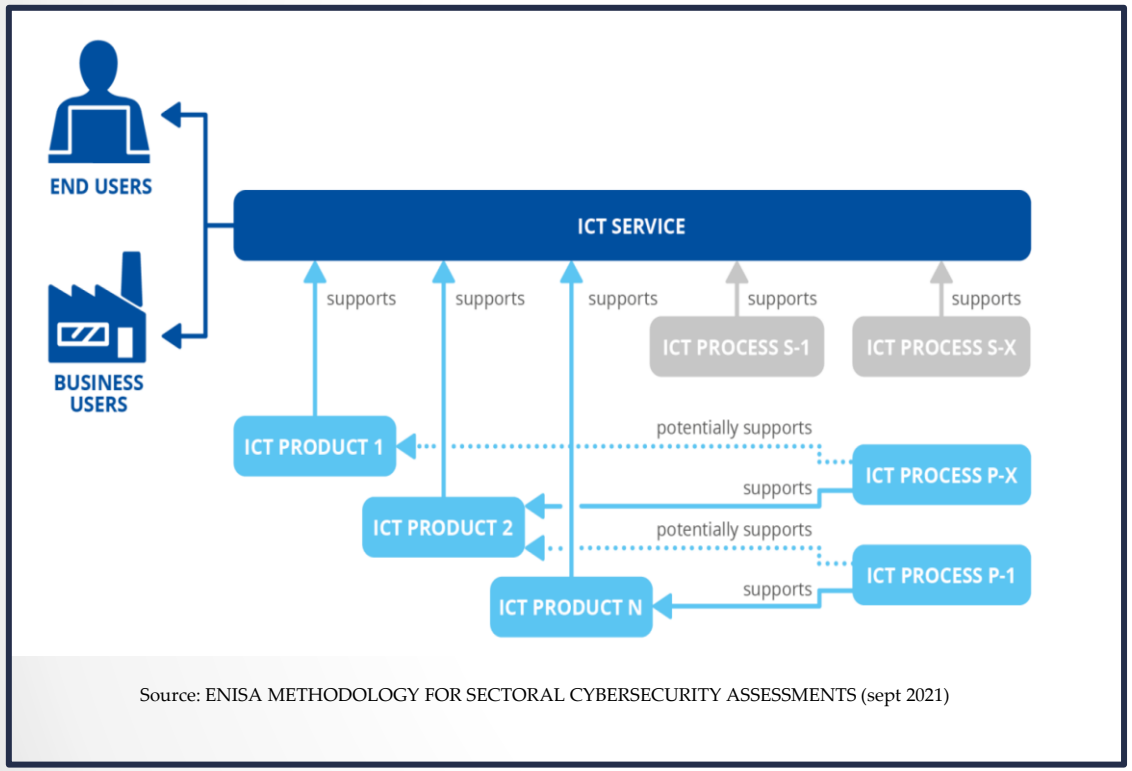
Article 25

Data protection by design and by default

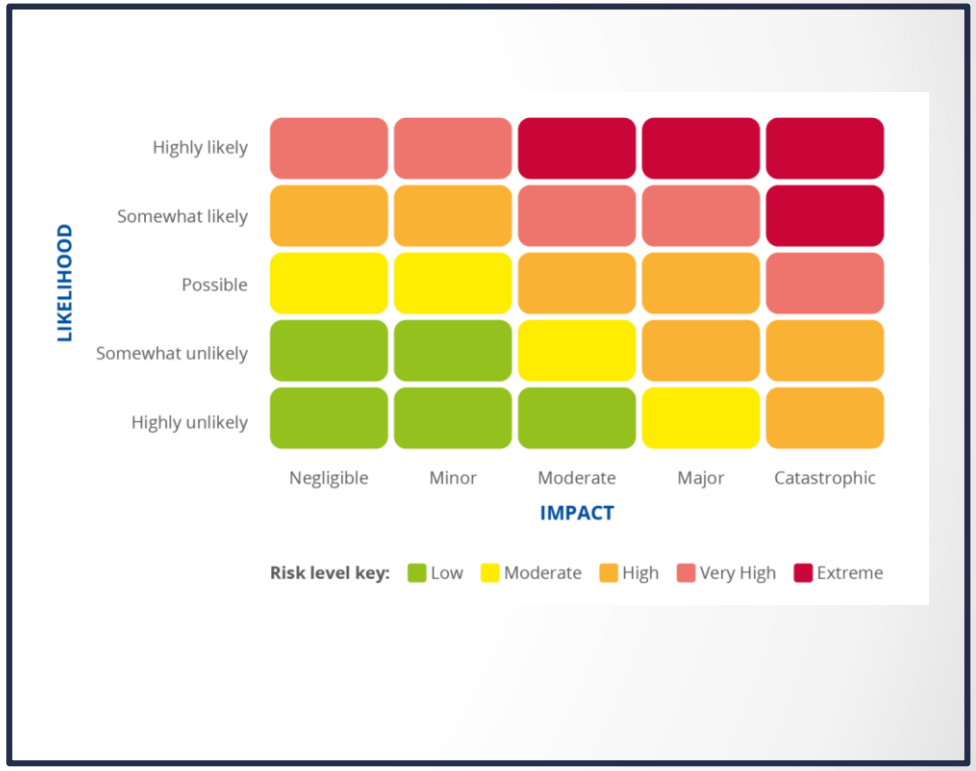
1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

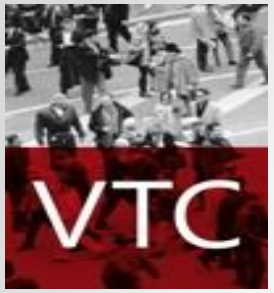
2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.



Source: ENISA METHODOLOGY FOR SECTORAL CYBERSECURITY ASSESSMENTS (sept 2021)

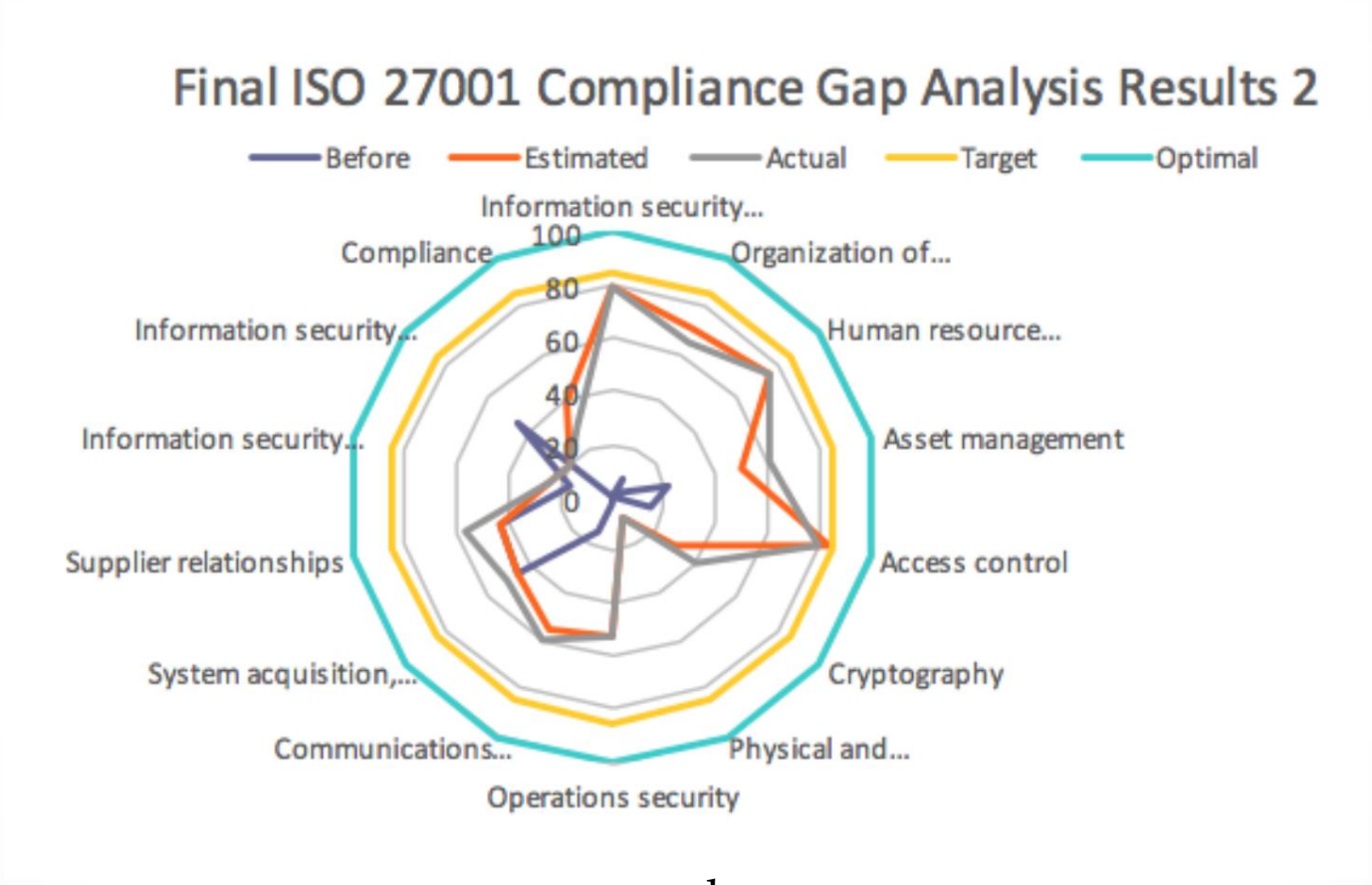




The 14 Domains of ISO 27001

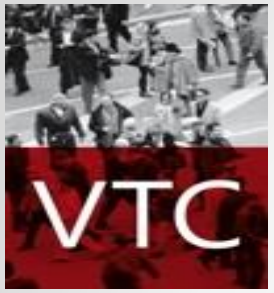
- Information Security Policies
- Human Resource Security
- Access Control
- Physical and Environmental Security
- Operations Security
- Organization of Information Security
- Asset Management
- Cryptography
- System Acquisition, Development, and Maintenance
- Supplier Relationships
- Communication Security
- Business Continuity Management
- Compliance
- Information Security Incident Management

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO


Final ISO 27001 Compliance Gap Analysis Results 2
Before
Estimated
Actual
Target
Optimal
Information security...
Organization of...
Human resource...
Asset management
Access control
Cryptography
Physical and...
Operations security
Communications...
System acquisition,...
Supplier relationships
Information security...
Information security...
Compliance
100
80
60
40
20
0

example

Toelichting adviezen



Cloudadvies VTC/A/2020/05

1. de technische en organisatorische beveiligingsmaatregelen moeten vooraf bepaald zijn en conform het **gevoeligheidsniveau** van de te verwerken informatie[7];
2. de technische en organisatorische beveiligingsmaatregelen moeten voorafgaand aan het in productie nemen **effectief aanwezig** zijn; het volstaat niet dat deze gepland zijn voor de toekomst;
3. processen/verwerkingen moeten duidelijk worden **geïsoleerd/gesegmenteerd**[8] om zodoende te kunnen bepalen welke processen wel/geen toegang krijgen tot bepaalde persoonsgegevens;
4. de technische en organisatorische beveiligingsmaatregelen moeten **op voorhand** worden **getest**. Het testen dient onafhankelijk te gebeuren (d.i. door een ander team dan deze die de toepassing heeft bedacht/gebouwd[9]). In deze test dient ook het risico op toegang door de cloudprovider tot persoonsgegevens expliciet te worden meegenomen;
5. alle datacenters waar de persoonsgegevens gehost worden, moet zich bevinden in een **EU lidstaat**[10];
6. bij elke externe hosting moet er een **recht op verificatie** (bijvoorbeeld via een audit) tijdens de loop van het contract bedongen worden. Ook hier is de bedoelde verificatie in de eerste plaats, maar niet uitsluitend, bedoeld om te verzekeren dat de encryptie en andere beveiliging niet te doorbreken is door of met medewerking van de cloudleverancier.

Cloudadvies VTC/A/2020/05

	Niet Europese leverancier*	Europese externe leverancier**	Belgische overheid	Intern Vlaamse Overheid
Grootschaligheid: veel data van veel personen (ook over projecten en beleidsdomeinen heen)	X	Encryptie of vergelijkbare maatregel + externe controle	Beveiliging + externe controle	Beveiliging + externe controle
Risicogevoelige personen	X	X (tenzij specifieke wetgeving)	Beveiliging + externe controle	Beveiliging + externe controle
Gegevens die een zware negatieve impact kunnen hebben	X	Encryptie of vergelijkbare maatregel + externe controle	Beveiliging + externe controle	Beveiliging + externe controle
Gevoelige gegevens sensu lato - niet grootschalig en - tijdelijk	Encryptie of vergelijkbare maatregel + externe controle	Encryptie of vergelijkbare maatregel + externe controle	Beveiliging + externe controle	Beveiliging + interne controle
Unieke identificatoren	X	Encryptie of vergelijkbare maatregel + externe controle	Beveiliging + externe controle	Beveiliging + interne controle
Andere personen/persoonsgegevens	Encryptie of vergelijkbare maatregel + externe controle	Beveiliging + externe controle	Beveiliging + interne controle	Beveiliging + interne controle

Cloudadvies VTC/A/2022/02

Minimale controleobjectieven:

1) de verwerking van data at rest

2) de verwerking van data in motion

3) de verwerking van data in use

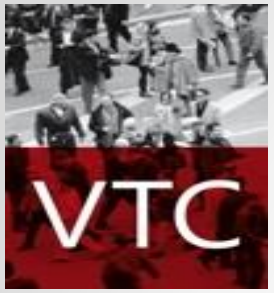
4) de beheersomgeving

5) het priviledged access management

6) secrets management en hardware security modules

7) gebruikers- en toegangsbeheer

8) audit trailing



VTC_A_2021_12_richtlijnen_kantoorpakketten

Volgende richtlijnen zijn bedoeld als houvast om te bepalen of het gebruik van algemene kantoorapplicaties in de publieke cloud AVG-conform is:

- **in principe niet aanvaardbaar voor** structureel dossierbeheer met persoonsgegevens. Daarvoor zijn specifieke applicaties met specifieke beveiliging vereist: de bedoelde kantoortoepassingen zijn daar niet voor bedoeld en de standaardbeveiliging is daar niet op afgesteld. Algemene kantoorapplicaties zijn niet bedoeld of geschikt als surrogaat voor een grootschalig verwerkingssysteem van persoonsgegevens;

- **in principe wel bruikbaar voor** het uitwisselen van ontwerpdocumenten zonder vertrouwelijke informatie en het uitvoeren van praktische taken, bv. samenwerken aan een beleidsplan. Daarbij kunnen incidenteel persoonsgegevens worden uitgewisseld, zoals de naam of het emailadres van een collega of beperkte informatie over de medewerker;

- **in principe niet aanvaardbaar voor** het delen of uitwisselen van gevoelige persoonsgegevens zoals het uitwisselen van vaccinatiestatus;

- **in principe geen** applicatie voor participatie van de burger bv. met gedeelde mappen in de cloud.

CONCLUSIE

In principe te gebruiken als algemene kantoortoepassing en niet voor dossierbehandeling. Doe de risicoanalyse per geplande verwerking.

Leverancier-evaluatie

!!! EX ANTE !!!

A&A	Audit and Assurance
AIS	Application & Interface Security
BCR	Business Continuity Mgmt & Op Resilience
CCC	Change Control and Configuration Management
CEK	Cryptography, Encryption and Key Management
DCS	Datacenter Security
DSP	Data Security and Privacy
GRC	Governance, Risk Management and Compliance
HRS	Human Resources Security

*** model-checklist under construction ***