

# Space for Trust

**Know Yourself, Your Supply Chain and Your Enemies**

Safety, Security & Resilience of Space-Based Assets, Spectrum, Ground Systems, Their Supply Chains, Stakeholders & Other Earthlings

**Arthur van der Wees**

Managing Director **Arthur's Legal, Strategies & Systems**, the independent, global strategic legal firm & knowledge partner, covering the unique combination of technology, strategy, impact, ethics & law focusing on (inter)national, regional and global strategy & policy aspects in this Digital Age

Expert Advisor to Public & Private Sector organisations within EU, EEA, UK, NATO allies and friends (Digital Ecosystems, Data, Digital Identity, IoT, AI, Robotics, Computing, Spectrum, Dynamic Attributes, Risk, Safety, Cybersecurity, Privacy, Trust, Dynamic Assurance, Digital Sovereignty, Accountability & Rule of Law)

Member of European Alliance for Industrial Data, Cloud & Edge (Leader of Digital Sovereignty Taskforce, Cybersecurity Taskforce & Common Trust Principles)

Project Leader, Ethics, Security & Advisory Board Member to 25+ European projects on Data, Trust, Security, Privacy, Ethics, Accountability & Risk in Digital Ecosystems

Expert Member of Expert Group of European Commission on B2B Data Sharing & Computing Continuum (Data Act)

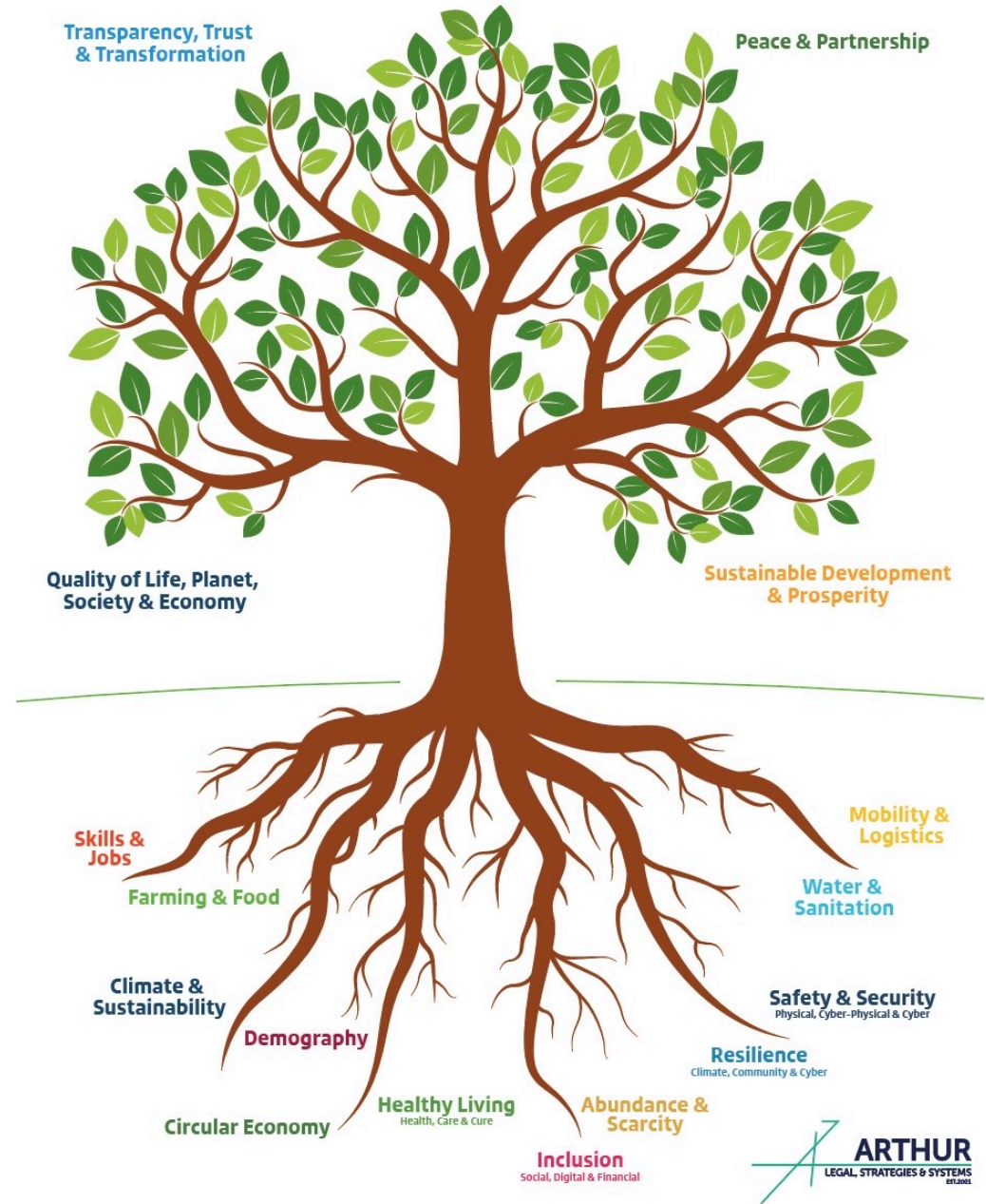


# Co-Creating Stellar Systems



# InterTwined Ecosystems

Powered by Purpose & Passion



# CONCORDIA National Stakeholder Group

## Focus Areas Priorities (2022)

EU Cybersecurity Industrial, Technology & Research Competence Centre, the Network of National Coordination Centres & Friends

**Demand- & Use-  
Procurement side**  
also within public sector  
organisations

**SMEs Demand-side**  
Awareness, Resilience & Digital  
Transformation

**Robust Upstream &  
Supply Chain Resilience**

**Awareness, Education,  
Training & Skills**

**Experts/Resource  
Pooling**  
Capacity Building

**Trusted Data Sharing**  
Data, Information &  
Knowledge, PPP-style

**X By Design & X  
By Implementation**  
in OT, IT, IoT & Data

**Sovereign Infrastructure  
& Work Space Resilience**

**Multi-Layered  
Governance**  
Strategic, Tactical &  
Operational

**Play to Win**  
No Reason To Go Alone

**Minimise Surprises**  
Grasping Importance

**Building Interdisciplinary**  
EU Communities &  
Ecosystems

Based on Chatham House Rule / Short, Mid & Long Term Priorities Combined



This project has received co-funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 830927.



# Space Sector is an Essential & Key Enabler

The Proliferation of the Space Sector Ecosystem reminds us of the early '90s of Internet 1.0

Commercialisation, Dependability & Opacity

Space Sector has a vast supply chain ecosystem, including more and more digital and data assets

In general, 30% of Economic Value in this ecosystem is created by SMEs (which is expected to increase)

However, being Valuable equals Getting Special Attention

# Anything that can be connected can get compromised

Space borne systems, such as communication satellites, navigation, sensory, earth observation, and a multitude of other functionalities, form an integral part of global communication, data processing, OT, IT & IoT – critical and other - infrastructures.

To date the interplay of Space and Cyberspace is underrated.

This part of our connected, inter-connected and hyper-connected world, which is a set of complex infrastructures and supply chain ecosystems, requires immediate, dedicated and continuous attention.

## #Systematic Risk

# Some Types of Threats & Vulnerabilities in Space Systems (Ground, Space & Network Segments) & their Supply Chain Ecosystem

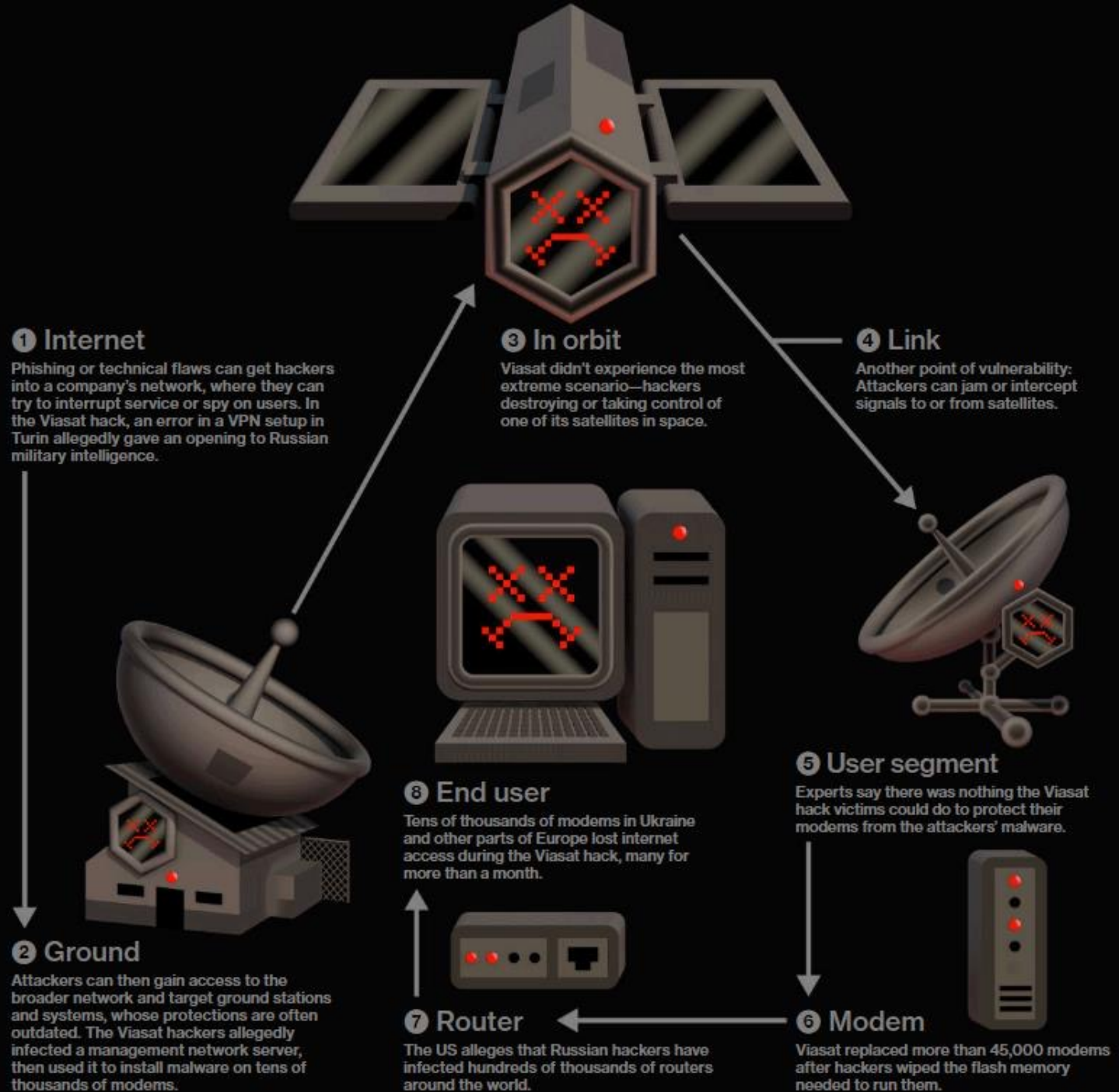
- A. **Access:** Cyberattacks and intrusions against ground systems and infrastructures supporting space operations as well as user applications and interactions.
- B. **KYS (Know Your Satellite):** Adversary using space situational awareness to target satellites, attack space assets with counterspace weapons, and assess the effectiveness of those attacks.
- C. **Lock out:** Adversary taking control of space assets in an unauthorized manner by operationally infiltrating and compromising satellites and locking out the legitimate satellite owners.
- D. **Inject:** Exploitation of the software and hardware vulnerabilities of the space assets.
- E. **Hijack:** Attacker altering the legitimate signals of a satellite and reusing it for another purpose.
- F. **Shadow:** Monitoring and tracking of military and other sensitive activities and locations on the earth using space assets such as surveillance satellites.
- G. **No Comm:** Adversaries conduct attacks to disrupt, deny, deceive, or degrade space communications, navigation and other services.
- H. **Too Much Comm:** Eavesdropping on satellite communications.

Security challenges when space merges with cyberspace, by Varadharajan & Suri (2023) <https://doi.org/10.1016/j.spacepol.2023.101600>

Cyber capabilities threaten **all** space segments.

Distinction as a non-government entity does **not** provide protection from adversary attack

USSF (2023)



# Space for Trust

**Know Yourself, Your Supply Chain and Your Enemies**

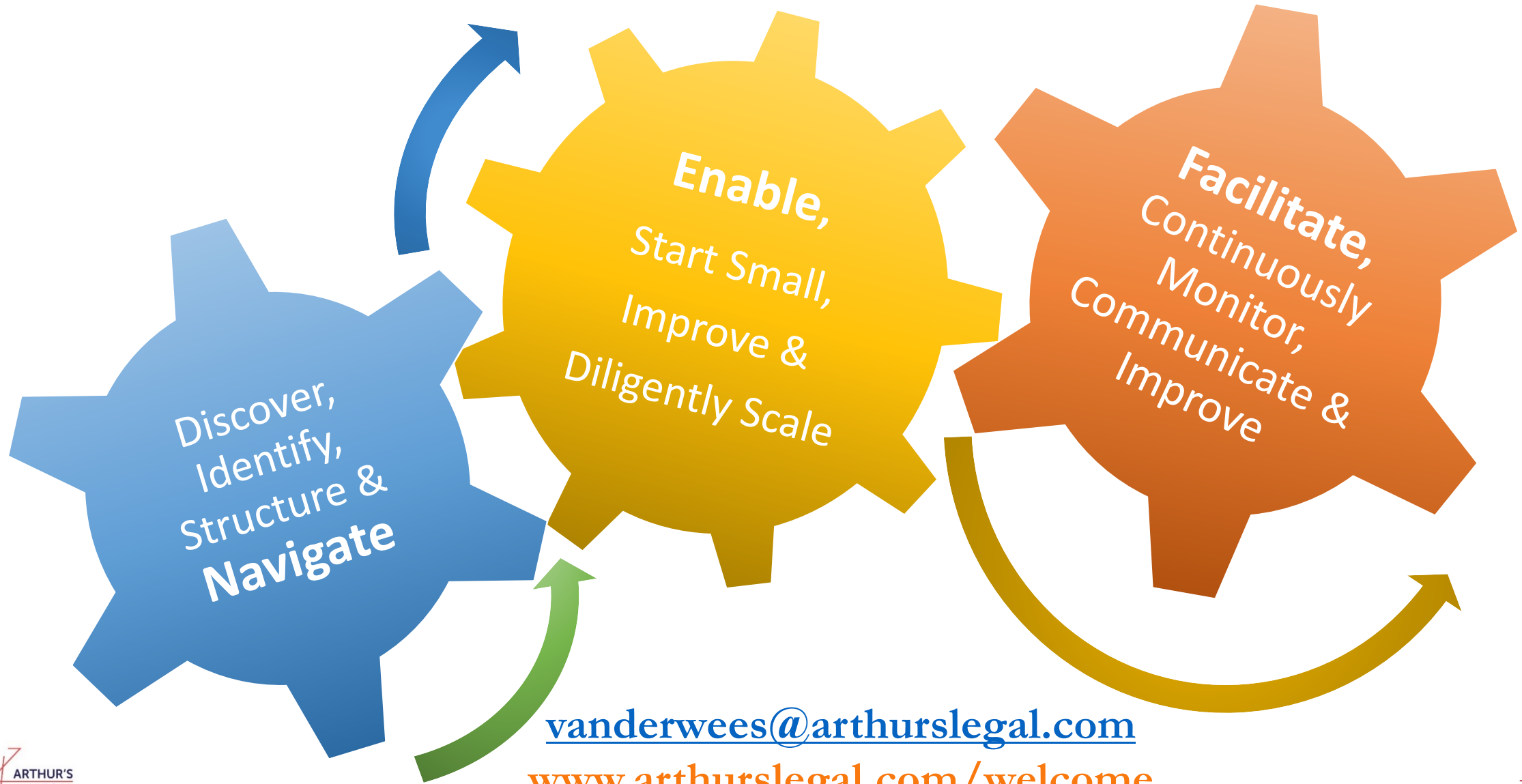
Find & Fix Deficiencies whether these Arise from Design,  
Operation, Dependencies, Law or Deliberate Instances

**Rethink Upstream, Midstream, Sidestream & Downstream**

**Trusted Data Sharing, Updatability & Resiliency**



# Our Vision, Mission & Mode of Operation



[vanderwees@arthurslegal.com](mailto:vanderwees@arthurslegal.com)

[www.arthurslegal.com/welcome](http://www.arthurslegal.com/welcome)

## Welcome to Arthur's Legal, Strategies & Systems

the independent, global strategic legal firm & knowledge partner, covering the unique combination of societal challenges, knowledge, technology, strategy, impact, ethics, law & trust focusing on (inter)national, regional, global and galactic strategy & policy aspects in this Digital Age

## Legal Notices

For use by 'Convergence 2023' Conference Participants of 30 November & 1 December 2023 in Brussels:



**Attribution-NonCommercial-ShareAlike 2.0 Generic (CC BY-NC-SA 2.0), Arthur's Legal B.V.**

For the other part: all rights reserved, Arthur's Legal B.V.

The content of this document is provided 'as-is' and for general information purposes only; it does not constitute strategic, legal or any other professional advice. The content or parts thereof may not be complete, accurate or up to date. Notwithstanding anything contained in this document, Arthur's Legal disclaims responsibility (including where Arthur's Legal or any of its officers, employees, contractors or partners have been negligent) for any direct or indirect loss, damage, claim, or liability any person, company, organisation or other entity or body may incur as a result, this to the maximum extent permitted by law.

Arthur Strategies & Systems is a tradename of Arthur's Legal B.V.