VISMA APPLICATION SECURITY PROGRAM AND CLOUD DELIVERY MODEL

This document provides Information about the Visma Application Security program and Visma Cloud Delivery Model intended for public distribution. The information in this document is identical to the information provided on https://www.visma.com/trust-centre/security/vasp-vcdm/.

Version 1.0, 08.04.2021.

Introduction **2**

An agile approach **4**

Privacy and data protection **5**

Which products are covered? **6**

Visma group policies and personnel **7**

Audits **7**

Design and Development **8**

Asset register 8

The Security Self-Assessment 8

Data protection and privacy 9

Use of third party data processors 9

Privacy by Design 10

Data Protection Impact Assessment 10

Risk Management 11

Risk Profile and Security Maturity 12

Risk Review 12

Risk Management 13

Tools and Services 13

Static Application Security Test (SAST) 13

Manual Application Vulnerability Assessment (MAVA) 14

Dynamic Application Security Test (DAST) 14

Automated Third Party Vulnerability Service (ATVS) 14

Security Log Management (SLM) 14

Cyber Threat Intelligence(CTI) 15

Operations **16**

The Maturity Indices 16

Product Security Operations Centre 16

The Trust Centre 16

The Visma Software Terms of Service 16

Bug Bounty and Responsible Disclosure 17

Introduction

It is important for Visma as a service provider to demonstrate to you, our customer, that our products and services are secure and protect your data and privacy, so that you may use them for your business purposes with trust and confidence.

Visma is a large corporation, with numerous products and services in many different markets and countries, and using different technologies. Our customers range from small businesses to large corporations and municipalities, in sectors ranging from plumbing to banking. The product in question can be Software as a Service (SaaS), locally installed at the customer's premises, a mobile app, or services such as electronic payment and invoicing, government reports and many other things.

In order to provide appropriate security and data protection across this spectrum, we've built a comprehensive security program for our products and services. This program is called the "**Visma Application Security Program**", abbreviated VASP.

VASP: A custom-made application security program

VASP is a custom-made application security program based on leading industry standards and best practices, and embedded directly into our production systems. It is a tiered and scalable program, where the requirements that a product has to comply with are tailored to the product in question; its technology, delivery model, market and other factors.

For instance, the requirements for a payroll system in the public cloud are different from an ERP system installed on a single customer's own hardware, which in turn are different from a mobile app.

The objective of the program is to ensure that our products are managed, developed and operated throughout its lifecycle in a secure and compliant manner with regards to application security, data protection and privacy, both for Visma as a provider and you as a customer.

VASP protects your security and privacy through organisational and technical measures, designed to protect the confidentiality, integrity, and availability of your data, and the resilience and legal compliance of our products and services. These measures are described in detail in the following chapters.

VCDM: An Information Security Management System for the cloud

For our cloud services, we have developed a full Information Security Management System (ISMS) certified on the ISO 27001- standard. An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information risk management processes.

Our ISMS is called "**Visma Cloud Delivery Model**". It shares many components with VASP, but has its own governance system and covers more than VASP, which is focused primarily

on application security and data protection:

VCDM is designed specifically for cloud delivery of software products, and therefore includes things like change management, problem management and release management. It also has additional controls, such for access management and security.

The VCDM framework describes our approach to developing, delivering and operating cloud services. It describes aspects of how we should be organized, how we should work (processes) as well as technical requirements and best practices necessary for successful cloud service delivery.

The model is based on a set of core principles and focuses on Devops and Continuous Delivery. VCDM is certified for ISO9001 and ISO27001.

Bringing it all together

This means that we have a two- tiered system, into which products are organised to a large extent based on technology:

Most legacy or on- premises systems, which are installed on the customer's machines, are following the Visma Application Security program, but our cloud services, where Visma is also responsible for the provisioning of the service in a cloud environment, are also following the Visma Cloud Delivery Model, with its additional and specialised requirements.

This document describes these two systems in great detail.

Please note however, that this document provides a summary of complex internal systems intended for public distribution. Its purpose is not to document every aspect of these systems, but to provide appropriate information for customers and prospective customers about how Visma works with application security and privacy compliance.

This means that certain parts of VASP and VCDM are purposefully omitted or only included by reference. For example, roles mentioned in this document, such as the Security Engineer and Data Protection Manager, have role descriptions in our Quality Management System that details their responsibilities, qualifications and authority. Similarly, most things pertaining to *governance* are not explicitly detailed here, such as onboarding processes to the programs, various group policies and change management of the programs. Similarly, references to Visma's internal organisation is omitted, because the programs are designed not to be affected by any internal re-organisation of Visma, in order to ensure the system's resilience.

You can also download this information in .pdf- format for your convenience and documentation. This may be a good idea to do at the time of purchase, as the document describes the program at that particular point in time. The document will always have a version number and date.

An agile approach

Within VASP and VCDM, we have a “bottom-up” approach to security and data protection. This means that rather than having a large, centralised security organisation with a lot of policies, reporting systems etc, we focus on the development teams:

The development teams are the software development and delivery teams that build and run the products you use. They are the ones who know the product best; its strengths, weaknesses and context in the market. The team is responsible not just for coding, but for the entire product all through its lifecycle, including things such as releases and security incident management. VASP (and VCDM) seek to empower the teams to provide the best possible security.

Every team has a dedicated “Security Engineer”. This is a specialised role described in our Quality Management System, just like other roles typically associated with a software company, such as “Developer” or “System Architect”. The Security Engineer receives additional training in security and data protection, and acts as the team’s specialist and primary point of contact on issues related to security and data protection. The Security Engineer works closely with the security team:

The development teams are closely supported by the Security Team. The Security Team is a team of dedicated application security professionals whose job it is to support and enable the development teams to assume responsibility for their product by providing expertise, guidance and certain tools and systems, such as threat intelligence, code scanning and support with security incidents.

The Security Team also provides training for the development teams, and maintains the Security Guild. The guild is where the Security Engineers interact and collaborate, organises training, shares information and expertise.

This approach, where the team itself is also responsible for security and operations, is often called “DevOps” or “SecDevOps”, and is a modern, holistic and agile approach to application security.

In sum, we believe that enabling and supporting the teams to take responsibility for "their product” yields a far better level of security than the more traditional approach of “write code and hand it off to Operations”, just as having our Security Team and Data Protection Manager working hands-on on a day-to-day basis with the teams is a far better use of their competence than having them monitor systems and writing reports and policies (they do that also).

Privacy and data protection

Privacy and data protection are critically important, particularly for our cloud services. Within VASP and VCDM, there are numerous requirements for privacy compliance that start right at the design- phase for a new product and carry through to its end- of- life.

These requirements are explained in greater detail in the next chapters, however, as part of this introduction we'd like to emphasise a couple of things:

In Visma, we draw a distinction between "security", "privacy" and "data protection":

Security, or more accurately in our context here: **application security**, is concerned with finding, fixing and preventing security vulnerabilities, in order to protect the assets in the application from threats and attacks.

These assets can be the application itself, but is in most cases *data*. Your accounting data, payroll and expense claims, user data, invoice information etc. Any data that you as a customer process using our products.

This means that application security, while based on a risk- assessment of the types or categories of data that are being processed by the application, does not primarily concern itself with how data is *used*, how it *can* be used or even *what* types of data it is. It focuses narrowly (and correctly!) on how to protect it.

This is where privacy and data protection comes in. "Privacy" in this context means the privacy protections afforded to *individuals* for their personal data through the GDPR, the General Data Protection Regulation. "Data protection" means the protection of customer data, such as accounting data, in an application *including* any personal data.

In a word, application security protects a container. Privacy and data protection is about what's inside the container.

Privacy and data protection focuses on the data itself:

- What type and categories of data is it?
- What is the legal basis for processing the data?
- What are the legitimate purposes for processing the data?
- Are there any particular risks associated with this type of data?
- Which rights and obligations does Visma, our customers and individual users have as a result of the types of data processed in our products?
- What security measures and functionality should the product support in order to meet these rights and obligations?

These and many other questions are the bread and butter of data protection. Within VASP and VCDM, we have split security and data protection into two separate but complementary domains through the independent role of the "data protection manager":

The Data Protection Manager (DPM) is a role modelled after the Data Protection Officer (DPO) role mandated by the GDPR. In the Visma group of companies, there is only one Data

Protection Officer, however, every legal unit in Visma has a DPM. The DPM acts as an advisor and contact point for matters related to privacy and data protection within his or her particular organisation in Visma.

Just like the DPO, the DPM is an independent position. This independence is crucial in enabling the DPM to act with a mind to protect the privacy and data of data subjects and customers in an appropriate manner. The DPM reports to management of his or her company, and to the DPO.

In VASP, the DPO is an important stakeholder for everything concerned with privacy and data protection within the program, and is also automatically notified of any security incident with a privacy or data protection impact.

Further, every Security Self-Assessment is reviewed by the DPO and/ or representatives of the DPO, which means that before any product is certified for either VASP or VCDM, it has to be reviewed by both security and the DPM. (More on the review process in the "Design and Development" chapter below).

Which products are covered?

You can check whether a particular product or service is following VASP, VCDM or other programs in Visma on the public Trust Centre:

https://www.visma.com/trust-centre/product-search/

Visma group policies and personnel

VASP and VCDM are security programs. However, in the Visma group of companies, there is an overarching security and privacy framework consisting of policies, guidelines and systems for managing everything from location access and device security to the use of subcontractors. The corporate security and privacy framework applies to all companies and units in Visma.

All Visma employees have confidentiality clauses in their employment contracts, and every employee also has to go through a mandatory e-learning course in privacy.

Audits

Both VASP and VCDM are audited annually by external auditors. The external audit includes both review of the Quality Management System and ISMS (VCDM), such as documentation, procedures and role descriptions, and interviews with teams and individual employees to verify that the system is followed.

All products in VASP and VCDM are subject to internal audits at least annually. These audits are performed by both a member of the security team and the DPO and/ or representatives of the DPO, to ensure that two different roles review the product before it gets “the green light”.

The purpose of the internal audit is to ensure compliance towards our Quality Management System and if applicable for the product in question, VCDM, and to identify areas of improvements for the product or service, the team and the security programs themselves.. Follow-up actions are registered and followed up in the Security Maturity Index, Architecture Index and if appropriate as risks.

Specifically for VCDM, internal audits are handled through the dedicated VCDM Compliance Process. This includes preparations, review meeting, review report, and registering follow ups that will be measured through the VCDM Index.

Design and Development

This and the following section, "Operations", describe the various main components and services that make up VASP. All these components and services are shared alike with VCDM.

Asset register

The entry- point into the Visma Application Security Program is the asset register. We call this the "Product Security Catalog", and it is a register over all assets (primarily software products) in the program.

The Product Security Catalog contains lots of information about the asset in question, such as its name, owner, who its security engineer is, and its status for the various services described below:

The Security Self-Assessment

The Security Self- Assessment, or SSA, is in many ways the heart of security, privacy and data protection in our products. The SSA consists of numerous requirements, recommendations and assessments for application security and privacy compliance, and is designed to provide:

- *Documentation* of how the product fulfils the *requirements* of the SSA, and;
- *Actions* that must or should be taken in order to *improve* security and compliance.

The SSA is a very detailed document, and is reviewed at least annually by both a member of the security team and the DPO and/ or representatives of the DPO. Having a current and reviewed SSA is also part of the VCDM approval process for products that are on the VCDM program (please refer to the introduction for an explanation of VCDM).

The output of an SSA is in the form of tickets in our development backlog system. We are a software company, and if something is not in the backlog, it does not exist. For example, if an SSA review concludes that a product should improve its encryption or client side input validation, a ticket is created and added to the development backlog.

The ticket is then associated with the SSA in the backlog system, in order to be measured in the Maturity Indices. Important tickets, and particularly tickets associated with risk for either the customer or Visma, are further prioritised through the embedded risk management system. This enables us to measure how well we fulfil the requirements and recommendations from the SSA, and also provides us with a risk- based approach to security and privacy.

While custom-made by Visma for Visma, the SSA is, by virtue of being an application security program, in many ways similar to industry best practices and frameworks, such as OWASP Top 10 and OpenSAMM.

Here are some examples from the Visma Security Self- Assessment:

- A **system diagram**, showing system components and interactions, including integrations and any external actors, such as hosting providers.
- A **list of data** that is processed by the application, or which the application is designed to process. (For example, names, contacts, document types, user preference information.)
- **Data classification** scheme, including categories of personal data, purposes for processing, and a rating for the data in terms of Confidentiality, Integrity and Availability ("CIA"; a common classification triad in information security, and also found in the GDPR).
- **Standards** or other requirements that may apply to the product, such as for payment services or the health and education sector.
- Numerous requirements for **Identity and Access Management (IAM)**, including permissions, security logging, 2- factor authentication and similar, **integrations**, **monitoring** and things like the use of encryption, secrets management and secure deployment.

In short, the SSA defines requirements and how we *should* meet them. How well we *actually do* are measured and followed up through the use of certain tools, processes and services and then presented in the maturity indices.

Data protection and privacy

The SSA contains a large chapter on data protection and privacy, which is reviewed separately and independently by the DPO or representative of the DPO.

The intention is to ensure that the product is compliant with applicable privacy laws and regulations such as the General Data Protection Regulation (GDPR), and also with our customer contracts.

Here are some examples:

Use of third party data processors

The Product Security Catalog and SSA contains controls and requirements for the use of a third party data processor in our service provision. This is typically third party hosting providers, such as Amazon Web Services or Microsoft Azure, but can also be third parties we use for service monitoring, customer feedback- and improvement or security purposes.

All third parties that process customer data and/ or personal data, are registered, including verification that the purpose for processing and processing location are legitimate and authorised. (And specifically, any use of third party data processors is checked against the Visma Software Terms of Service.)

This process also determines if a data processing agreement is required, and if so, one is entered into with the third party data processor.

Privacy by Design

Privacy by design is a set of principles for designing and operating software that broadly speaking can be said to implement the principles for data protection, such as data minimisation, limited data storage periods and purpose limitations.

The GDPR states specifically that the data controller should adopt internal policies and implement measures which in particular meet the principles of data protection by design and data protection by default ("privacy by design" for short here) in order to be able to demonstrate compliance with the regulation.

This makes privacy by design very important for Visma as a service provider too. We have implemented about thirty non-functional requirements, guidelines and/ or recommendations that have been adopted specifically for software development based on the recommendations provided by the data inspectorate.

These are categorised as:

- Purpose, minimisation and proportionality
- Data deletion
- Data export and return
- Data restore
- Customer guidance
- Automated decision making
- Pseudonymisation and anonymisation
- Consent from data subject

These requirements and recommendations range from the simple "does the application process only the minimum personal data required to function" and whether roles in the system can be configured to only have access to relevant data, to more complex and particular requirements for the deletion of data when a customer relationship is terminated, and methodological guidelines for various anonymisation- techniques.

Data Protection Impact Assessment

The Data Protection Impact Assessment, or DPIA, is another requirement that follows from the GDPR, which states that the data controller shall carry out an assessment of the potential impact of the processing of personal data if such processing is likely to result in a high risk to the rights and freedoms of natural persons.

Further, the GDPR states that the data processor (Visma in most cases) should assist the controller (you as the customer in most cases) where necessary. To this end, we have created a detailed template for DPIA suitable for a software product, and criteria to determine if a DPIA is needed for a particular product or processing activity.

The DPIA template is structured as follows:

- Description of the processing, such as:
    - Legal basis for processing

    - Scope, duration and nature of the processing
    - Recipients, systems and tools to be used for the processing
    - Compliance with customer contracts
- Accountability
    - Responsible parties
    - Advice of the DPO
- Necessity and proportionality
    - Specified, explicit and legitimate purposes for processing
    - Necessity of the processing
    - Data minimisation
    - Storage limitation
- Measures contributing to the rights of data subjects
    - Information to data subjects
    - Publication of main findings
    - Right of access, erasure etc, and the right to object
    - Prior consultation
- Risk assessment
    - Threats or sources of risk
    - Potential impact to the rights and freedoms of data subjects
    - Risk assessment

Risk Management

How do we decide what level of security a particular product should have? How do we determine by what mechanisms, technologies or measures we achieve that level of security?

The answer is partly in the above; in our security requirements, standards, procedures and guidelines, which are designed to ensure a certain security baseline and common practices. However, these cannot tell us what is appropriate for a particular product in a particular environment or context (whether technical, geographical or with regards to the threat environment, or the type of the data it processes).

For example, what level of security should we have for an international cloud payroll system, for an on-premise ERP system, a mobile expense app, a system for handling boardroom activities or even a bank integration? What are the risks of unwanted or unauthorised destruction, misuse or disclosure of data for each product? What are the threats against each product?

The answer to these questions are determined through risk assessments. The risk assessment aims to determine which technical and organisational measures are required in order to ensure a level of security that is *appropriate* to the risk represented by the processing of data (customer data and personal data), having regard to the *context* of the product in question.

Specifically within VASP and VCDM, this is done as follows:

Risk Profile and Security Maturity

Every product is classified into risk categories based on factors such as what types of and the extent of data it processes, the state of its technology, which markets it operates in and what threats we see through our intelligence services.

The first step in the SSA is to complete the "risk profile". We sometimes call this "inherent risk", because these are risks that we cannot wholly mitigate or reduce, because they are inherent to a particular market or activity. For example, a system processing financial data has a different risk profile than one processing health information. We also look at the categories and volume of data, and certain technological factors such as whether the system is deployed in a cloud environment.

As a result of its risk profile and other factors, each product is assigned a minimum Security Maturity tier. This further ensures a minimum level of security based on the general or "inherent" risk of operating the system.

The idea behind assessing the inherent risk first, is that the team is aware of this as they progress through the rest of the SSA, before arriving at the risk assessment at the very end:

Risk Review

Before an SSA is successfully reviewed and passed by both security and data protection, a risk review is conducted.

This goes through the now completed SSA, including all tickets that were created (for fixing or improving things), as well as information from security incidents if any, threat intelligence and other sources such as the various tests and tools described in the next chapter, in order to identify potential sources of risks in the product within its own context; environment, data, customers, technology etc.

Please note that these are not narrowly defined or technical risks only, but also general and high level risk. If for example the Data Protection Officeris not satisfied with the privacy by design, he or she can also register a risk, and is indeed obligated to do so.

Risks are registered for processing in our risk management system:

Risk Management

The VASP and VCDM Risk Management system is as simple as it is effective: it is built directly into the same backlog system we use to process other tickets from the SSA, and indeed any development backlog issue. The risk management system however uses its own dedicated security scheme in order to ensure the confidentiality of any risk tickets, and also has its own risk- specific workflow.

The methodology is the now very common *risk = impact x likelihood* methodology, with risk, impact and likelihood levels appropriate to Visma and our customers. In addition, the definition of risk includes information about the **asset** and/ or **data** being protected, its **value**, **vulnerabilities** and **threats** against it.

Once a risk is registered, it escalates up the management chain depending on its criticality and risk acceptance power schedules.

Visma firmly believes that risk management is a management responsibility.

If action is required by the product team in order to address the risk, the issue is assigned back to the team with instructions and a priority, and it flows back into the backlog.

The result is an appropriate level of security, which is based on both a general and specific risk assessment.

Tools and Services

Static Application Security Test (SAST)

SAST is a service designed to analyse the source code of Visma services to identify Security defects. It integrates in the CI/CD (Continuous Integration/ Continuous Delivery) pipeline for full automation and with our ticketing system for export of details. It also integrates with notification systems to ensure that the developers get information in a timely manner.

The system provides triage functionality for defects in order to classify severity and actions.

The SAST service is put in place to reduce the risk of costly security incidents due to implementation defects in source code at an early stage in the process while the root cause is faster to fix. Parts of SAST are automated, and integrated in the build process as well as ticketing and source code management systems.

The SAST service also provides good training for developers and teaches how to avoid making security defects.

Manual Application Vulnerability Assessment (MAVA)

The manual application vulnerability assessment is in-house dynamic gray-box application level manual security testing service. Testing is done in a pre-production environment (usually staging) with authentication credentials to test companies provisioned by the development teams.

The service is designed to identify application level weaknesses and vulnerabilities, most of which are covered in OWASP Top 10. Some of the findings may be infrastructure related, such as TLS configuration, web server errors, exposure of sensitive files. Most findings are discovered during authenticated testing. Usually several sets of credentials on at least a couple of different tenants are required for a test to uncover missing function level access control, and cross tenant isolation flaws.

For each web application we perform our baseline security tests as a minimum and technology specific tests on top of that depending on the situation.

Dynamic Application Security Test (DAST)

Dynamic Application Security Testing (DAST) is a process of testing an application or software product in an operating state. DAST works by sending mock attacks to web applications and services via HTTP/HTTPS, just like a cybercriminal would.

DAST requires little knowledge of an application's inner workings, and findings inherently provide proof of exploitation that demonstrates whether an application is indeed vulnerable and how that vulnerability can be exploited.

The results are triaged by the security team.

Automated Third Party Vulnerability Service (ATVS)

Automated Third Party Vulnerability Service (ATVS), also sometimes referred to as SCA, Software Composition Analysis, is a way of detecting and managing known third-party vulnerabilities in any open source components used.

Open source components such as frameworks and libraries are commonly used in software, and these may have known vulnerabilities that require to be patched or updated. This service assists in prioritizing components to be updated.

ATVS also assists in license compliance for these components, such as for the use of open source libraries.

Security Log Management (SLM)

We have established a common security log management process for our cloud based products to ensure that Visma is in the best possible position to detect, investigate and prevent cyber crime, fraud and other threats towards our customers and our services. This also helps us to verify our own compliance to data protection legislation such as GDPR.

Cyber Threat Intelligence(CTI)

Cyber Threat Intelligence Service is a service providing intelligence on threats to our systems using certain research and monitoring capabilities.

Operations

The Maturity Indices

The Maturity Index is an internal tool used to measure the live status of a product in various areas such as Security, UX (User Experience), Architecture and Technology, and VCDM. It allows strengths and weaknesses to be identified over time for each product, and is used to prioritise development in terms of security and data protection.

In a word, the Security Self-Assessment tells us what we *should* be doing. The index tells us if we're *actually* doing it.

Product Security Operations Centre

The security professionals in the Product Security Operations Centre handle all our security systems and frameworks, day-to-day security operations (incident management for instance) and also provide training and guidance to our product teams in all matters related to security.

The operations centre is capable of running operations over time, round the clock, when and if required.

The Trust Centre

The Trust Centre is the Visma group's public web pages for information about privacy and data protection in Visma. All the information in this document is replicated there.

The Trust Centre also includes detailed information about specific products and services, such as any data processors involved in the service provision.

The Visma Software Terms of Service

The Visma Software Terms of Service (TOS) is the standard terms of service for numerous products and services from Visma.

The TOS came about in 2018, when the General Data Protection Regulation (GDPR) necessitated that Visma entered into new data processing agreements with all its customers. In anticipation of this, we formulated the data processing agreement in the TOS and entered the requirements from that into the then- version of the SSA (for instance with regards to purpose limitations).

This ensured that our customer contract was GDPR- compliant when the GDPR came into effect, and indeed only products that fulfilled the requirements of the security program were allowed to use the TOS as its contract.

This is still the case, and will always be the case.

The TOS confers many other advantages, particularly for the customer, because it is a single agreement for many different products. This means that instead of entering into one agreement per product or service, the TOS applies to all products that fulfil the requirements set forth in VASP or VCDM.

This means that everything from your right of use to intellectual property clauses, and in particular the data processing agreement, are the same for all these products, and you can be sure that there is back- to- back compliance between the TOS and VASP/ VCDM, and also between all the products and services you use.

I.e. the TOS is not a stand- alone legal text, or a text that is compliant with the law but disconnected from technical and organisational security measures. The TOS is built on top of the Visma Application Security Program, and only products that are compliant with the program use it.

Bug Bounty and Responsible Disclosure

Bug Bounty is a great and proven way of “battle testing” the security of a service with ethical hackers around the world paid to report security vulnerabilities to us. This program is meant to complement the Visma Application Security Program (VASP) and is a partnership with Intigrity, one of Europe’s biggest platforms for such purposes.

In this program, we encourage external security professionals and ethical hackers to search for security bugs in our products and report them to us.

If the reporters follow the policy (or rules of conduct) that we have published, we will reward them with money for every valid bug they report. In this way, we increase the chances that friendly testers will report bugs, which allows us to fix them before they are found and abused by cyber criminals.

We have two levels of bug bounty programs. A "private" program, used by around 150 specifically invited testers, and a "public" program, available for several thousands of testers. For both programs, we have only specific assets that are in scope and only those are eligible for bounties.

The strength of a Bug Bounty program lies within the number of eyes and expertise because more researchers means more findings and better security.

Responsible Disclosure Program is an extension of the Bug Bounty program where all the Visma assets are in scope. We invite security researchers to find vulnerabilities and report them to us and provide transparent rules for them:

https://www.visma.com/trust-centre/security/products-and-services/bug-bounty-and-responsible-disclosure/

In this case, we do not offer monetary rewards, but as a sign of appreciation, for valid reports, we offer them a place in our Hall of Fame:

https://www.visma.com/trust-centre/security/products-and-services/bug-bounty-and-responsible-disclosure/hall-of-fame/

End of document.