Unofficial translation Government Gazette

Order of the Minister of Foreign Affairs of (Date), nr.BZ26(number), laying down administrative rules and a ceiling for grants awarded under the Ministry of Foreign Affairs Grant Regulations 2006 (Grant Programme Netherlands – Ukraine cybersecurity)

The Minister of Foreign Affairs,

Having regard to articles 6 and 7 of the Ministry of Foreign Affairs Grants Decree;

Having regard to articles 2.4, subsection f, of the Ministry of Foreign Affairs Grant Regulations 2006;

Orders:

Article 1:

The administrative rules appended as an annexe to this Order apply to grants awarded under articles 2.4, subsection f, of the Ministry of Foreign Affairs Grant Regulations 2006, with a view to supporting activities that contribute to the cybersecurity in Ukraine, from the date on which this Order enters into force up to and including 31 December 2030.

Article 2:

1. Grant applications in the scope of the Grant Programme Netherlands – Ukraine cybersecurity may be submitted from 9:00 CET on 2 April 2026, until 17:00 CET on 29 April 2026.

2. Grant applications under the Grant Programme for Netherlands- Ukraine cybersecurity must be submitted using the application form made available by the Minister and must be accompanied by the documents stipulated in that form[1].

Article 3:

1. For the Grant award in the framework of the Grant program 'the Netherlands – Ukraine Cybersecurity' described in Article 2, paragraph 1, for a period from in effect till 31 December 2030 with a total of a grant ceiling of €2,5 million subcategorised in following grant ceilings:
a. € 625.000 for solutions that simplify or improve solutions for the implementation of Security Operations-Centre-as-a-Service and Managed Security Service Providers;
b. € 625.000 for Cloud-security solutions which contribute to a diversification of cloud-storage and services in Ukraine;
c. € 625.000 for solutions that contribute to the improvement of Identity and Access Management and e-mail protection, in order to promote the integrity of data;
d. € 625.000 for developments which optimize forensic investigation and incident response.
2. If a grant ceiling, laid down in Paragraph 1, subcategorised a up until d, is not fully utilised for which it was determined, the remaining amount will be made available for applications aimed at the grant ceiling with the most applications.

Article 4

The division of the ceiling for grants, laid down in article 3, will take place based on the criteria that are set out in the annexe of this decision, which outlines that from the applications that meet the

[1] www.rvo.nl/subsidies-financiering/nl-ua-cf

criteria, the best assessed will firstly qualify for grant awarding, within the framework that evenly spreads of available tools laid down in Article 8, paragraph 3, part d, of the grant decision of the Ministry of Foreign Affairs.

Article 5

This Order enters into force on the day after the date of the Government Gazette in which it appears and lapses with effect from 1 January 2031, with the proviso that it continues to apply to applications submitted and grants awarded prior to that date.

Article 6

This Order will be referred as: Grant Programme Netherlands – Ukraine Cybersecurity.

This Order and its accompanying annexe will be published in the Government Gazette.

The Minister of Foreign Affairs,
For Director-General of Political Affairs,
M. de Vink

ANNEX

1. Background

In recent years, due to strong increase since the start of the Russian invasion, a significant number of cyberattacks are occurring on all layers of the Ukrainian government. These attacks affect the health care sector, financial institutions, the business sector and the vital infrastructure of Ukraine. Russian cyber offenses are inseparably connected to the war and worsens the daily life of many Ukrainians. Ukrainian authorities and the complete cybersecurity ecosystem work daily with all their manpower available to strengthen cybersecurity.

Simultaneously, European countries, including the Netherlands, also are hindered by the increase of cyberattacks, according to reports of the National Coordinator for Counterterrorism and Security (NCTS) and the National Cybersecurity Centre (NCSC) [2]. The Netherlands must be prepared for an increased number of cyberattacks on government actors in the near future. Dutch parties have significant knowledge and expertise in cybersecurity and have a remarkable reputation in means of innovation at the international stage.

Currently, in regards to cybersecurity, many exchanges are occurring between Dutch and Ukrainian government actors. This exchange does not occur as much between cybersecurity enterprises from both countries. However, there is a mutual strong desire to learn from one another. Dutch enterprises would like to prepare for an uncertain geopolitical future and are willing to learn how cyber defence works at the frontline of Ukraine. Likewise, Ukrainian enterprises have a significant interest in specific skills of the Dutch ecosystem and innovative ideas that could be applied in their daily work.

The Tallinn Mechanism[3] is established in 2023 to coordinate civil cybersecurity support of multiple countries to Ukraine. Priorities under the Tallinn Mechanism are increasing the resilience of the Ukrainian cybersecurity ecosystem, the coordination of financial support to Ukraine, and stimulating business-to-business relations between Ukrainian enterprises and countries that are member of the Tallinn Mechanism. The Dutch government ordered on 16 July 2025 decided to facilitate 20 million euro for the support of cybersecurity in Ukraine for 2025 and 2026.[4]

1.2 Contributions to priorities of the Tallinn Mechanism
Given the ongoing huge necessity of support from Ukraine, in combination with the status of national security in the Netherlands, the minister will contribute with the Grant program Netherlands-Ukraine cybersecurity (hereafter: grant program) to the goals that were set for the Tallinn Mechanism. The Grant program is established to connect the Ukrainian and Dutch private sector, with a focus on the added value to the Dutch private sector.

The cybersecurity ecosystem in Ukraine has a lot to endure under the constant Russian attacks. The necessity is high in many areas of cybersecurity, deriving from the delivery of Security Operations Center (SOC) services to the protection of critical data. Innovative products could reduce the pressure and allow cybersecurity providers to work more efficiently.

The minister will make tools available via the Grant Program for projects of partnerships of Dutch and Ukrainian enterprises which contribute to civil cybersecurity purposes in Ukraine. Military cybersecurity purposes therefore do not fall within the reach of this grant.

The Netherlands strives to align as good as possible to the priorities of the Ukrainian cybersecurity community, with regard to cybersecurity and the connection of the Ukrainian ecosystem to the Dutch ecosystem. Dutch enterprises have significant expertise in many aspects of the cybersecurity

[2] https://www.nctv.nl/documenten/2025/11/26/cybersecuritybeeld-nederland-2025
[3] https://www.government.nl/documents/diplomatic-statements/2023/12/20/tallinn-mechanism-officially-formalized
[4] kst-36045-209.pdf

sector. Facilitating the delivery of a short-term contribution of the (Dutch) private sector will therefore be deemed in achieving increased cybersecurity in Ukraine and the Netherlands.

For illustration purposes hereafter will follow a description of the type of projects that the Grant program aims to finance:

- Solutions which simplify or improve the implementation of SOC as-a-service and Managed Security Service providers. Think of tools and onboarding methods;
- Cloud-security solutions which contribute that Ukraine can diversify with regard to providers of cloud storage and services, and which are in line with the European movement to a sovereign cloud. The proposed cloud solutions must have a strong security level and guarantee a high level of availability;
- Solutions that contribute to the improvement of Identity and Access Management and e-mail protection, for the promotion of integrity of data;
- Developments that will optimize forensic investigation and incident response. Think of scripts / guidelines, tabletop exercises for crisis preparation, and tools which simplify or improve forensic investigation.

2. Implementing Organisation

The Minister has mandated the Netherlands Enterprise Agency (RVO), an agency of the Ministry of Economic Affairs and Climate, to implement this grant programme. The Netherlands Enterprise Agency (RVO) will carry out this grant programme on behalf of the minister on the basis of an issued the Netherlands Enterprise Agency (RVO) mandate.

3. Definitions

The following definitions are used in this grant programme:
- *Economic activity:* any activity in which goods or services are offered on a market;
- *Group:* a group is an economic entity, wherein organizational are connected:
a. an entity with legal personality governed by private law that directly or indirectly:
    1° holds more than half of the issued share capital of,
    2° is a fully liable partner of, or
    3° has a controlling interest in
    one or more legal persons, and
b. the latter legal person/persons;
- *Tax group*: a group of businesses seen as one business for tax purposes
- *Civil society organisation*: a non-profit organisation that is not connected to a government organisation either de facto or under its constitution, which serves a public interest and possesses legal personality, and is registered as such – it must not have been established by a government organisation, or must have become fully autonomous from the government organisation that established it;
- *Minister:* the Minister of Foreign Affairs;
- *Business*: a legal person carrying out economic activity, which is not a trade association, knowledge institution or civil society organisation;
- *Consortium:* a contractual partnership without legal personality, whose partners themselves each have legal personality under civil law, that is aimed at achieving common objectives by carrying out activities, such that each partner delivers part of the necessary input and bears part of the accompanying risks.
- *Consortium leader:* member of the consortium that applies for the grant on its behalf – if the application is approved, the consortium leader is the grant recipient and as such bears full responsibility towards the Minister for implementation of the grant-funded activities and compliance with the obligations in respect of the grant;

4. Grant Programme the Netherlands - Ukraine cybersecurity

4.1 Objective and target audience

The objective of the grant programme is to increase the collaboration between the Ukrainian and Dutch cybersecurity ecosystem, allowing Dutch entrepreneurs to learn from Ukrainian cybersecurity, and to contribute to civil cybersecurity in Ukraine, as described in paragraph 1.

4.2 Parties that may be eligible for a grant:

With the grants in this program the minister intends to support partnerships, on behalf of which the consortium leader will apply for a grant.

The partners and partnership must meet the following requirements:

- Each partner is an enterprise;
- The partnership must consist of two businesses, from which one is a local registered Ukrainian business that has knowledge of the local context, and at least one business that is registered in the Netherlands;
- Each partner has demonstrable expertise in the type of activities as described such as those to which the activities to be carried out by the party within the set framework related to the partnership;
- Each partner has demonstrable structural guaranteed and sufficient capacity to carry out the activities by the party within the set framework related to the partnership;
- All partners must be necessary to achieve the objective of the activities for the applied grant by a demonstrable and significant role within the partnership to fulfil, which is evident from the project plan;
- The partnership must be established before the grant application.

The role of the consortium leader will be fulfilled by a business registered in the Netherlands or a business registered abroad and an establishment or permanent seat in the Netherlands. Furthermore it is required by the consortium leader that:

- A minimum of 3 FTE[5] employed/ full-time employees[6], which must be demonstrated by requesting the documents that must be submitted (such as a collective wage statement), wherein a case of a group of fiscal unity this group is considered to be for the group of fiscal unity
- Has demonstrable ability to manage finances adequately to ensure the targeted and effective implementation of activities.

Ukrainian and Dutch (semi-)government institutions are not eligible for a grant in the framework of this grant program (not directly as party lead nor as partner in the partnership). It is, however, possible to involve these institutions as (members of) the consortium, on which they can advise on local needs in order to achieve the targets.

4.3 Eligible activities

To be eligible for a grant under this programme, the application must describe a coherent and comprehensive set of activities (‘project’) aimed at achieving and contributing to the shared objective.

The project has to centre around *one* of the following domains corresponding to the grant ceilings into which the complete grant ceiling available for dispersion of funds within the framework of this grant programme, is divided:
a. € 625.000 for solutions that simplify or improve solutions for the implementation of Security Operations-Centre-as-a-Service and Managed Security Service Providers;

[5] "FTE" stands for "full-time equivalents". The calculation of FTEs varies by company or social organisation, but is generally calculated by dividing the number of hours worked by an employee by the number of hours of a full working week.
[6] https://www.belastingdienst.nl/wps/wcm/connect/nl/arbeidsrelaties/content/wanneer-is-sprake-van-loondienst

b. € 625.000 for Cloud-security solutions which contribute to a diversification of cloud-storage and services in Ukraine;
c. € 625.000 for solutions that contribute to the improvement of Identity and Access Management and e-mail protection, in order to promote the integrity of data;
d. € 625.000 for developments which optimize forensic investigation and incident response.
2. If a grant ceiling, laid down in Paragraph 1, subcategorised a up until d, is not fully utilised for which it was determined, the remaining amount will be made available for applications aimed at the grant ceiling with the most applications.

Furthermore, the project:

- Contributes to the objective laid down in paragraph 4.1.
- Responds to local needs in Ukraine;
- Keeps the connection with the correct Ukrainian partner(s) into account and contributes to a substantial transfer of knowledge between the consortium partner(s), evident by the task division and the plan of action for knowledge exchange;
- Connects to Dutch and European needs for cybersecurity solutions and the increased level of threat, appearing from references to European legislation such as the NIS2[7] and the CRA[8], to threat- images or reports from the NCSC and the NCTV, or references to an adjusted corporate strategy or adjusted priorities as a result of the war in Ukraine.
- Ensures that solutions that contribute to the improvement of civil cybersecurity in Ukraine by using local Ukrainian data which can be implemented easily by end users, for example by the integration of current cybersecurity platforms;
- Suits within the long-term cyber resilience strategy of the Dutch partner;
- Is cost-efficient in relation to the desired results and predicted risks;
- Must be realistic and attainable in the designated duration, concluding in the described goals and the demonstrable experience of the partners in the consortium;
- Has drawn up mitigating measures for the identified risks that could hinder the execution of the project.

In any case, activities for which a grant or contribution has already been received directly from the (Dutch) Ministry of Foreign Affairs are not eligible for funding

4.4 Duration of activities:

The activities for which a grant is requested have a maximum duration of 6 months. Activities must start within one month of the grant award.

4.5 Size of the grant

Grants will be awarded for up to 100% of the eligible costs, with a minimum grant amount per application of €200,000 and a maximum of €250,000. Only if there are remaining funds from a grant ceiling for one domain that are allocated to applications for another domain (see section 7.1 for further details) may a rewarded grant be less than €200,000, but at least €125,000.

5. Eligible costs

5.1 Principles

The following principles apply when determining the costs (and the extent thereof) that may be taken into account in determining the amount of the grant to be awarded:

- Costs must be reasonable, logical and necessary.[9]
- The activities must, by their nature, be suitable for the partner incurring the costs.
- Costs must be directly related to carrying out the activities and must not include contingencies.

[7] European NIS2-regulation (Regulation (EU) 2022/2555),
[8] European Act Cyberresilience (Directive (EU) 2024/2847).
[9] See also article 14 of the Grant decision Ministry of Foreign Affairs

- Only costs incurred after the application is submitted are eligible for a grant.
- Internal costs are eligible without mark-up.
- Costs will be compared with local standards and assessed for reasonability..
- Costs relating to project management and coordination, may not exceed 10% of the total eligible costs.

5.2 Eligible costs

The following costs to be incurred by the partners are eligible for a grant:

a. Staff costs: the number of hours worked by people directly involved with the eligible activities, multiplied by no more than €87.50, which should include both direct wage costs and associated indirect costs, up to a maximum of €700 a day.
b. Depreciation of assets, with the exception of land and existing buildings, during the course of the activities. The basis for determining the depreciation costs is the purchase price, taken into account the eventual residual value plus eventual adjustment costs. If assets, with the exception of land and existing buildings, are transferred following the cessation of activities to an organization in Ukraine that is not part of the transferring partner's tax group, the acquisition cost of these assets may be increased by the eligible costs.
c. Third party costs: costs payable to third parties, supported by an invoice, with a maximum of 10% of the total grant received.
d. Travel costs: international travel costs and interregional travel costs outside the Netherlands based on economy class fares.
e. Subsistence costs: the maximum compensation for subsistence costs is the number of overnight stays multiplied by the accommodation- and other costs conform the Daily Subsistence Allowance Rates of the United Nations[10], applicable at the moment of application. Additionally, extra travel- and subsistence costs may be eligible due to risks, insurances and negative travel advice, provided that it is well substantiated in the application

5.3 Costs not eligible for a grant

The following costs are in any event not eligible:

- the costs of developing and submitting the grant application as well as other costs made for the submitting of the application;
- value-added tax (VAT), in so far this is not a cost item
- financing costs and interest payments;
- costs resulting from inflation and exchange rate fluctuations;
- licensing fees;
- costs for the purchase of property and existing buildings
- costs of registering, maintaining and protecting intellectual property rights;
- contingencies.

6. Application

6.1 Requirements

The application must be submitted using the tool provided for this purpose by RVO and must include the annexes specified therein, for which templates are provided by RVO. The project plan, the budget and the cooperation agreement must be submitted in English. The supporting documents for a minimum of 3 FTEs in salaried employment for the consortium leader may be submitted in Dutch or English.

The application must in any event include:

- Proof that the company has at least 3 FTE on its payroll (e.g. a collective wage statement), which, in the case of a group or fiscal unity, applies to the group or fiscal unity as a whole
- Project plan, which meets the requirements laid down in paragraph 4.4 and contains at least:

[10] https://icsc.un.org/Home/DailySubsistence

- An elaborated description of the activities, in which it becomes clear for which domain the grant application applies;
- A description of the initial situation prior to the activities;
- The expected results of the project including the contribution to the priorities and (sub)objectives of this grant programme, as mentioned in paragraph 4.1.;
- Delineation of the project;
- A justification on how the activities respond to local needs in Ukraine and connect to the policy/priorities of the Ukrainian government related to cybersecurity;
- A description of the collaboration between the partners which explains why each partner is necessary to the implementation of the project for which the grant was applied (each partner has a demonstrable, active and significant role within the consortium);
- A description of the collaboration with and between the most important stakeholders;
- A description of local parties (beneficiaries) which will receive knowledge and/or goods including a substantiated description of their role in and contribution to the project, if applicable;
- A justification on how the partners are able to implement the project in means of the war situation and the complex Ukrainian context;
- A risk analysis with an overview of the most important risks related to the project with the associated mitigating measures, by which can be thought on the following risks:
  - Implementation risks in a war situation;
  - Financial implementation risks;
  - Risks related to safe business practices;
  - Risks of corruption;
  - Other risks applicable to the project;

- Budget for the total project costs;
- Signed consortium agreements which guarantees the cooperation of the partners to the implementation of the activities and guarantee task division and compliance by the partners of the mutual agreements, as well as compliancy to the minister on the grant dedicated obligations.

The applicant shall ensure that each business participating in the application declares that it is aware of, and will act in accordance with, the OECD Guidelines.[11] This means that companies apply due diligence in accordance with these guidelines to identify (potential) negative impacts on people and the environment in their own activities and their value chain, address them where necessary, and communicate transparently about this. Companies also declare that they do not engage in activities listed on the FMO Exclusion List.[12]

Companies must immediately report to RVO any signals or circumstances indicating involvement in a violation of the OECD Guidelines, including violations of human rights or significant environmental damage. If a report has been (or is to be) submitted regarding a company to the Dutch National Contact Point (NCP) for the OECD Guidelines[13], companies must report this to RVO and cooperate with the NCP.

6.2 recovery period

In the context of the application procedure, emphasis is placed on article 7, paragraph 3, of the Grant decision of the Ministry of Foreign affairs. In case an application is filed incompletely, the minister could (with the use of article 4:5 of the General Administrative Law) request additional information. Date and time of receipt of application will be validated as the new date and time on which the additional information is received.

In this regard, the closer to the deadline of the submitting the application, the risk that the minister will not grant the opportunity to use his authority to request additional information

[11] https://www.oesorichtlijnen.nl/
[12] https://www.fmo.nl/policies-and-position-statements
[13] https://www.oesorichtlijnen.nl/meldingen

increases; this relates to the time that will be consumed with checking all applications on completeness and the time that is needed to ask for additional information. In that instance, the application cannot therefore be completed and will be assessed how it was submitted at first instance. This can lead to a rejection of the grant application.

Furthermore, in general submitting an incomplete or insufficient substantiation of (parts of) the application may lead to a rejection of the grant application based on the failure to comply or insufficient compliance to the requirements and criteria.

When filling in the form, it is not sufficient to refer for the sake of brevity to other parts of the application, websites or annexes, unless the application form states that this is wholly or partly acceptable. Incomplete applications may be rejected.

7. Assessment of applications and allocation of resources

7.1 Assessment and allocation

The provisions of the General Administrative Law Act, the Ministry of Foreign Affairs Grants Decree and the Ministry of Foreign Affairs Grant Regulations 2006 are fully applicable to the assessment of applications and the award of grants under this grant programme. Applications will be assessed in accordance with the above legislation and pursuant to the requirements set out in this grant programme.

To be eligible for a grant, applications must satisfy the requirements set out in sections 4 to 6. Only applications that meet those requirements will proceed to an assessment of their quality based on the criteria set out in paragraph 7.2. These criteria must be met to a sufficient degree (at least 63 points out of a maximum of 95) in order to be eligible for a grant. Criteria 1 through 3 must also achieve at least a minimum number of points in order to qualify for a grant; see section 7.2 for further details.

The allocation of grant funds for each of the grant ceilings/domains (see section 4.3) takes place through a grant tender, i.e., on the basis of quality. Quality is assessed by evaluating applications based on the qualitative criteria set forth in Section 7.2. Applications are evaluated by the domain under which they are submitted. The results of this evaluation lead to a ranking of the applications per grant ceiling/domain based on quality. Applications that do not meet at least a satisfactory quality standard will not be included in this ranking.

In the event that approving two or more applications with equally high scores would result in exceeding the grant ceiling for the domain to which the applications relate, a lottery will be held to determine which application is approved.

If grant funds remain from a grant ceiling for a domain, these funds will be made available for applications in the domain for which the most applications have been submitted. In this case, the minimum grant amount is €125,000.

7.2 Criteria

The following criteria are applicable to the contribution of the goal laid down in paragraph 4.1. The allocation of points depends on the extent to which these (sub-) criteria are matched.

There is a maximum of points that can be achieved per criteria 1 to 3 and their designated sub-criteria. Bonus points can be earned under criteria 4.

Caution: In case only the minimum points of criteria 1 to 3 are obtained, the grant will not be allocated because only 57 points are obtained. For allocation of the grant the proposal should obtain a minimum of 63 points. This means that more points than the minimum must be obtained for criteria 1 to 3, or the discrepancy can be compensated with the bonus points from criteria 4, or the proposal can use a combination of both options.

Criteria	Maximum points
1. Alignment of needs and priorities (minimum 20 points)	
1.1 The degree to which the consortium partners are suitable to implement the project, evident from the presence of the required competences and expertise so that the project; a. responds to the needs of Ukraine, and b. uses the knowledge of the partners.	10
1.2 The extent to which the project adheres to one of the following four themes and the consortium has proven expertise in implementing such projects and the implementation domain of the development or developing method or technique: • Solutions that simplify or improve the implementation of SOC-as-a-Service and Managed Security Service Providers; • Cloud security solutions that contribute that Ukraine can diversify with regard to cloud-storage and service providers. The solutions must be in line with the EU shift to becoming a sovereign cloud. The proposed cloud solutions must have a high level of security and guarantee a high level of availability. • Solutions that contribute to the improvement of access policy and offering guarantees with regard to integrity of data by innovative and flexible solutions of Identity and Access Management and e-mail protection; • Developments that optimize forensic investigation and incident response.	10
1.3 The extent of sufficient transfer of knowledge and capacities between both parties in the consortium, under which is understood an adequate division of the labour and a plan for regular knowledge exchange between the partners, based on interests and needs from both parties.	10
2. Results and impact (minimum 17 points)	
2.1 The extent to which the project contributes to improve civil cybersecurity in Ukraine, evident from a description of how the project connects to Ukrainian needs, the use of local data, the fast implementation of solutions in a volatile environment and the integration of the solution into existing cybersecurity platforms	10
2.2 The extent to which a project contributes to the creation of long-term cybersecurity solutions which can be utilized in Ukraine and/or the Netherlands, connecting to the themes set out in criteria 1.2 and developed with references to relevant cybersecurity policy objectives, mentioned in Dutch, Ukrainian or European documents, as described in section 4.4.	10
2.3 The extent to which the project's results will be incorporated into future cybersecurity plans of Dutch companies, as evidenced by references to current and future European and Dutch cybersecurity legislation and business objectives, as described in section 4.4.	5
3. Plan of action and efficiency (minimum 20 points) The extent to which the quality of the project plan and the budget is guaranteed, as shown by:	
3.1 The extent to which the project is cost-efficient, in which there will be looked to the height of the (eligible) costs in relation to the expected development results and risks.	10
3.2 a) The project plan has been drafted specific, measurable, attainable, realistic and time-bound (SMART), b) objectives are realistic and concrete, c) the scope which illustrates the expertise of the consortium in comparable projects.	10
3.3 a) The extent to which risks are identified for achieving the envisaged project results, and b) to the extent of specification of risks in what manner mitigation occurs.	10

4. Extra points (no minimum)	
4.1 The extent to which a project has a clear plan for future cooperation between the Dutch and Ukrainian partners when the project finishes	5
4.2. The extent to which the Dutch party of the consortium has demonstrable prior experience with working in Ukraine since February 20, 2014	5
Total number of points (minimum 63 and maximum 95 points)	

In aid of its assessment, RVO may undertake action to verify any assumptions or statements made in the application. To this end, it may obtain the information needed to properly assess the quality of the application.

8. Grounds for rejection

In addition to the provisions of Section 4:35 of the General Administrative Law Act, an application for a grant will be rejected if the requirements of this grant scheme are not met or if the available grant funds are insufficient. An application will also be rejected if the project focuses (in part) on military cybersecurity.

9. Impact of war

If an ongoing project is hindered by the Russian invasion, so that it suffers damage or cannot be fully completed, the grant recipient will report this in accordance with the terms of the grant award. The grant recipient will then consult RVO to jointly seek out a reasonable solution. The project could be temporarily suspended until the situation improves, could be fully suspended, or otherwise. If the decision is taken jointly to suspend the project, the remaining grant must be reimbursed, in case an excess of advances has already been received. The grant recipient is responsible for the safety risks in Ukraine.[14]

10. Monitoring

RVO will carry out random checks and, where possible, monitor the correct use of the grant, verifying its legality and effectiveness on the basis of the decisions issued.

11. Obligations

The grant decision will set out obligations tied to the grant recipient in the following:
- The obligation to notify of the facts and circumstances that may have a significant impact on the grant, such as the applicant's temporary or incomplete inability to implement activities for which a grant is awarded, as well as complying with OESO-guidelines.
- Forbids using child and/or forced labour[15]. The grant recipient must immediately notify RVO of any facts or circumstances that would suggest these organisations are using child and/or forced labour.
- Must deliver a final report after the termination of the project.

[14] https://www.nederlandwereldwijd.nl/reisadvies/oekraine.

[15] Any form of labour which the International Labour Organisation seeks to prevent through the Convention concerning Forced or Compulsory Labour, 1930 (C29), the Convention concerning the Abolition of Forced Labour, 1957 (C105), and the Convention concerning the Minimum Age, 1973.

12. Administrative burden

A test based on a standard cost model has been carried out in the interests of accountability for the administrative burden that the applicant will face, from drafting and submitting the application to the management phase, the determining of the definitive grant amount, and any objection and review procedures. The calculation shows that the administrative burden expressed as a percentage of the total available grant budget is 2.88%.