FFG
Forschung wirkt.

AUSSCHREIBUNG 2023, VERSION 1.2
EINREICHFRIST: 15.04.2024
DATUM: WIEN, 15.01.2024

CYBER SECURITY SCHECKS 2023
AUSSCHREIBUNGSLEITFADEN

INHALTSVERZEICHNIS

1 DAS WICHTIGSTE IN KÜRZE 4

2 ZIELE DER AUSSCHREIBUNG 5

3 DIE BASIS FÜR EINE FÖRDERUNG 5
3.1 Was sind Cyber Security Schecks? 5
3.1.1 Welche Projekte werden unterstützt? 6
3.1.2 Welche Technologien und Beratungen werden gefördert? 6
3.2 Wer ist förderbar? 8
3.3 Wie hoch ist die Förderung? 9
3.4 Welche Kosten sind förderbar? 9
3.5 Was ist hinsichtlich Projektlaufzeit zu beachten? 10
3.6 Information und Beratung zu NIS2 10

4 DIE EINREICHUNG 11
4.1 Wie verläuft die Einreichung? 11
4.2 Wie dürfen vertrauliche Projektdaten verwendet werden? 12

5 DIE BEWERTUNG UND DIE ENTSCHEIDUNG 13
5.1 Wie erfolgen die Bewertung und die Entscheidung? 13
5.2 Nach welchen Kriterien werden Förderungsansuchen bewertet? 14

6 DER ABLAUF DER FÖRDERUNG 15
6.1 Der Cyber Security Scheck in 5 Schritten 15
6.2 Welche Berichte und Abrechnungen sind erforderlich? 15
6.3 Wie erfolgt die Auszahlung der Förderung? 16
6.4 Wie müssen Änderungen kommuniziert werden? 17

7 RECHTSGRUNDLAGEN 17

8 WEITERE FÖRDERUNGSMÖGLICHKEITEN DER FFG 18

TABELLENVERZEICHNIS

Tabelle 1: Eckpunkte der Ausschreibung.....4
Tabelle 2: Förderbare KMU und Sektoren.....8

1 DAS WICHTIGSTE IN KÜRZE

Der Fond Zukunft Österreich und das Programm Digital Europe der Europäischen Kommission unterstützen zu gleichen Teilen die Ausschreibung **Cyber Security Schecks 2023**, eine Maßnahme des Nationalen Koordinierungszentrums für Cybersicherheit (NCC-AT), das das BKA in Kooperation mit der FFG leitet.

Tabelle 1: Eckpunkte der Ausschreibung

Eckpunkte	Informationen
Kurzbeschreibung	Cyber Security Schecks unterstützen KMU, die in den Anwendungsbereich der NIS2-Richtlinie fallen, bei der Umsetzung von technischen Sicherheitsmaßnahmen im Bereich der Cybersicherheit
Förderungshöhe	Max. 10.000 EUR pro Scheck Max. 1 Scheck pro Unternehmen
Förderungsquote	Max. 40 %
Förderungszeitraum	12 Monate ab Projektstart, keine Projektverlängerung möglich
Förderwerbende	Kleine und mittlere Unternehmen (KMU), die in den Anwendungsbereich der NIS2-Richtlinie fallen, mit Niederlassung in Österreich
Förderbare Kosten	Kosten für Technologien sowie Kosten für Beratungsleistungen zu Cybersicherheit
Budget gesamt	Max. 2 Mio. EUR
Einreichfrist Antrag	Einreichzeitraum 1: 16.10.2023 – 15.01.2024, 12:00 Uhr Einreichzeitraum 2: 15.01.2024 12:00 Uhr – 15.04.2024, 12:00 Uhr
Einreichfrist Endbericht	Innerhalb eines Monats nach Ende des Förderungszeitraums
Sprache	Deutsch
Ansprechpersonen	**Ausschreibungs-Management:** MMag. Erich Herber, T (0) 57755-2716; E erich.herber@ffg.at Mag. Josef Scheucher, T (0) 57755-2311; E josef.scheucher@ffg.at
Information im Web	https://www.ffg.at/ausschreibung/cybersecurityschecks2023

Eckpunkte	Informationen
Zum Einreichportal	https://ecall.ffg.at

2 ZIELE DER AUSSCHREIBUNG

Durch die NIS2-Richtlinie, die bis zum 17. Oktober 2024 umzusetzen ist, müssen viele Unternehmen verpflichtende Sicherheitsmaßnahmen und Meldepflichten im Bereich der Cybersicherheit implementieren. Ziel der Richtlinie ist es, auf europäischer Ebene ein hohes gemeinsames Cybersicherheitsniveau sicherzustellen. Einen wichtigen Bestandteil dieser Sicherheitsstrategie stellt die Stärkung der Resilienz und Reaktionsfähigkeit von Unternehmen gegenüber Cyberbedrohungen dar.

Mit der Ausschreibung **Cyber Security Schecks 2023** werden österreichische KMU in bestimmten Sektoren, die in den Anwendungsbereich der NIS2-Richtlinie fallen, mit einer Förderung bei der Umsetzung der dafür erforderlichen Sicherheitsmaßnahmen unterstützt. Damit soll eine Sensibilisierung für die durch die nationale Umsetzung der NIS2-Richtlinie entstehenden verpflichtenden Sicherheitsmaßnahmen erreicht und die Vorbereitung für betroffene KMU darauf erleichtert werden.

Der Fond Zukunft Österreich und das Programm Digital Europe der Europäischen Kommission unterstützen zu gleichen Teilen die Ausschreibung **Cyber Security Schecks 2023**, eine Maßnahme des Nationalen Koordinierungszentrums für Cybersicherheit (NCC-AT), das das BKA in Kooperation mit der FFG leitet.

Der vorliegende Leitfaden spezifiziert die Bedingungen für die Ausschreibung **Cyber Security Schecks 2023**.

3 DIE BASIS FÜR EINE FÖRDERUNG

3.1 Was sind Cyber Security Schecks?

Cyber Security Schecks unterstützen **österreichischen KMU im Anwendungsbereich der NIS2-Richtlinie** (vgl. Kapitel 3.2 und Kapitel 3.6) dabei, die Sicherheit und

Cyberabwehrfähigkeit ihrer Netz- und Informationssysteme zu stärken und die rechtlichen Anforderungen in diesem Zusammenhang zu erfüllen.

3.1.1 Welche Projekte werden unterstützt?

Mit der Förderung werden Unternehmen unterstützt, die im Rahmen des geförderten Projekts konkrete **technische Sicherheitsmaßnahmen** umsetzen, um die Sicherheit und Cyberabwehrfähigkeit ihrer Netz- und Informationssysteme zu stärken. Gefördert werden Kosten für die dafür erforderlichen **Technologien** sowie für **Beratungsleistungen zu Cybersicherheit**.

Die Projekte müssen geeignet sein, die **Anforderungen der NIS2-Richtlinie** zu erfüllen und auf **mindestens einen** der folgenden **Zwecke** ausgerichtet sein:

- Risikoanalyse und Sicherheit für Informationssysteme
- Bewältigung von Sicherheitsvorfällen
- Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall und Krisenmanagement
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen
- Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit
- grundlegende Verfahren im Bereich der Cyberhygiene
- Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung
- Sicherheit des Personals, Zugriffskontrolle und Management von Anlagen
- Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme im Unternehmen

Es werden ausschließlich Projekte gefördert, die **innerhalb von 12 Monaten ab dem Projektstart umgesetzt und abgeschlossen** werden (vgl. Kapitel 3.5).

3.1.2 Welche Technologien und Beratungen werden gefördert?

Gefördert werden **Technologien (Hardware und Software)**, die für die Umsetzung der technischen Sicherheitsmaßnahmen im Bereich der Cybersicherheit geeignet sind und zu diesem Zweck in die digitale Infrastruktur **integriert** werden.

Förderbar sind **Neuanschaffungen sowie erforderliche Upgrades** von Technologien.

Förderbare Technologien können beispielsweise umfassen:

- Server- und Netzwerktechnologien, Firewall-Systeme, Speichergeräte, Sensoren zur Überwachung von Netzwerkaktivitäten

- Softwareprodukte wie Sicherheits- und Verschlüsselungssoftware, Server- und Netzwerkbetriebssysteme sowie Cloud-Software mit Fokus auf Sicherheitsfunktionen, Künstliche Intelligenz zu Cybersicherheit

Bitte beachten Sie:

- Hardware, die zur üblichen IT-, Office- und Arbeitsplatzausstattung gehört, wie Desktop-Computer, Laptops, Smartphones, Kameras oder Audiogeräte, ist nicht förderbar.
- Sicherheitssoftware, die vorrangig für die Absicherung von Endgeräten ausgelegt ist, ist nur förderbar, wenn diese in einem Komplettpaket zur Umsetzung einer geplanten technischen Sicherheitsmaßnahme enthalten ist.

Zusätzlich werden **Beratungsleistungen zu Cybersicherheit** gefördert, die für die Umsetzung der technischen Sicherheitsmaßnahmen erforderlich sind.

Diese können beispielsweise umfassen:

- Konzeption und Design zum Auf- und Ausbau von Sicherheitsarchitekturen
- Technische Sicherheits- und Risikobewertung, inklusive Validierung
- Integration und Konfiguration geeigneter Sicherheitstechnologien
- Statusanalyse und Strategieberatung zur ganzheitlichen und systematischen technischen Umsetzung der NIS2-Richtlinie
- Produktschulungen für die Inbetriebnahme und Nutzung der im Rahmen des Projekts angeschafften Technologien (Hardware und Software)

Nicht förderbar sind beispielsweise:

- Beratungsleistungen ohne spezifischen NIS2-Bezug, z.B. generelle Management- und Rechtsberatung, DSGVO Beratung
- Beratung bzw. sonstige Leistungen in Verbindung mit der Entwicklung und Wartung von Technologien (beispielsweise Hardware-/Softwareentwicklung)
- Messebesuche, Konferenzteilnahme, Aus- und Weiterbildung

Bitte beachten Sie:

- **Art und Zweck** der Technologien bzw. Beratungsleistungen sowie ihr **Beitrag zur Umsetzung der NIS2-Richtlinie im Unternehmen** müssen im Antrag plausibel beschrieben werden, andernfalls sind diese nicht förderbar.
- Gehen Sie bei der Beschreibung Ihres Vorhabens vollständig und präzise auf die **Fragen** im **eCall Antragsformular** ein.
- Technologien und Beratungsleistungen können von **ausländischen Organisationen** zugekauft werden.

3.2 Wer ist förderbar?

Förderbar sind ausschließlich

- **Mittlere Unternehmen (MU**) – das sind Unternehmen bis 249 Beschäftigte und bis 50 Mio. EUR Jahresumsatz oder bis 43 Mio. EUR Jahresbilanzsumme, und
- **Kleinunternehmen (KU)** – das sind Unternehmen bis 49 Beschäftigte und bis 10 Mio. EUR Jahresumsatz oder Jahresbilanz,

die nicht der österreichischen Bundesverwaltung angehören und

- über eine **Niederlassung in Österreich** verfügen, und
- in den **Anwendungsbereich der NIS2 Richtlinie**[1] fallen, und
- einem der in Tabelle 2 dargestellten **Sektoren** gemäß Anhang I und Anhang II der NIS2-Richtlinie angehören (abhängig von der Unternehmensgröße).

Tabelle 2: Förderbare KMU und Sektoren

Unternehmensgröße	Sektoren
Mittlere Unternehmen (MU)	– **Sektoren mit hoher Kritikalität** (gem. Anhang I der NIS2-Richtlinie): Energie; Verkehr; Bankwesen; Finanzmarktinfrastrukturen; Gesundheitswesen; Trinkwasser; Abwasser; Digitale Infrastruktur; Verwaltung von IKT-Diensten (Business-to-Business); Weltraum – **Sonstige kritische Sektoren** (gem. Anhang II der NIS2-Richtlinie): Post- und Kurierdienste; Abfallbewirtschaftung; Produktion, Herstellung und Handel mit chemischen Stoffen; Produktion, Verarbeitung und Vertrieb von Lebensmitteln; Verarbeitendes Gewerbe/Herstellung von Waren; Anbieter digitaler Dienste
Kleinunternehmen (KU)	– **Sektoren mit hoher Kritikalität** (gem. Anhang I der NIS2-Richtlinie): Digitale Infrastruktur, Verwaltung von IKT-Diensten (Business-to-Business) – **Sonstige kritische Sektoren** (gem. Anhang II der NIS2-Richtlinie): Anbieter digitaler Dienste

Es wird empfohlen, Beratung zu NIS2 in Anspruch zu nehmen, um die Erfüllung dieser Voraussetzungen vor Antragstellung eingehend zu prüfen. Mögliche Informations- bzw. Beratungsangebote zu NIS2 finden Sie im Kapitel 3.6.

[1] RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)

Bitte beachten Sie zusätzlich:

- **Die Förderung ist eine De-minimis-Beihilfe** (vgl. Kapitel 7). Förderbar sind nur Unternehmen, die mit dem Förderungsansuchen bestätigen können, dass ihre Förderungen aus De-minimis-Beihilfen die zulässige Obergrenze nicht überschritten haben. Beachten Sie den Geltungsbereich der De-minimis Verordnung und darin gelistete Ausnahmen. Weitere Informationen
- Bezüglich der **Unternehmensgröße** ist die geltende KMU-Definition gemäß EU-Wettbewerbsrecht ausschlaggebend. Bei der Einstufung der Unternehmensgröße werden Unternehmen, die Beteiligungen an anderen Unternehmen (z.B. Mutter- und Tochterunternehmen) haben, als ein Unternehmen gewertet. Weitere Informationen
- **Ein-Personen-Unternehmen (EPU)** sind förderbar, wenn sie die Anforderungen dieser Ausschreibung erfüllen.
- **Unternehmen in Gründung** sind **nicht förderbar**.

Die FFG behält sich vor, Förderwerbende wegen Unvereinbarkeit auszuschließen.

3.3 Wie hoch ist die Förderung?

Die Förderung erfolgt in Form von nicht rückzahlbaren Zuschüssen und beträgt pro Cyber Security Scheck **maximal 10.000 €**. Die Förderquote beträgt **maximal 40 %** der förderbaren Gesamtkosten des Projekts.

Beispiele zur Berechnung der Förderhöhe:

- Bei 8.000 EUR Kosten werden max. 40% gefördert, also 3.200 EUR.
- Bei 20.000 EUR Kosten werden max. 40% gefördert, also 8.000 EUR.
- Ab 25.000 EUR Kosten tritt die Deckelung von max. 10.000 EUR in Kraft.

In dieser Ausschreibung kann **maximal 1 Cyber Security Scheck pro Unternehmen** gefördert werden.

Ein Cyber Security Scheck ist weder übertragbar, abtretbar, noch in Geld ablösbar.

3.4 Welche Kosten sind förderbar?

Förderbare Kosten sind alle dem Projekt zurechenbaren

- **Sachkosten für Technologien:** unter diese Kostenkategorie fallen Kosten für Neuanschaffungen und Upgrades von Technologien (vgl. Kapitel 3.1.2),
- **Drittkosten für Beratungsleistungen:** unter diese Kostenkategorie fallen Kosten für zugekaufte Beratungsleistungen (vgl. Kapitel 3.1.2),

die **direkt, tatsächlich und zusätzlich** (zum herkömmlichen Betriebsaufwand) während des Förderungszeitraums entstanden sind.

Bitte beachten Sie:

- Es können nur Kosten abgerechnet werden, die anhand von Belegen **nachweisbar** sind.
- Die zugekauften Leistungen müssen **im Förderungszeitraum** erbracht werden.
- Die Zahlung zugekaufter Leistungen muss auf Verlangen **mit Kontoauszug belegt** werden.
- Die geförderten Kosten dürfen nicht zusätzlich über andere Förderungen abgerechnet werden (**Verbot von Mehrfachförderungen**).
- Bei **vorsteuerabzugsberechtigten** Unternehmen wird die Umsatzsteuer nicht als förderbarer Kostenbestandteil anerkannt.

Für **Sachkosten** gelten zusätzlich folgende Bedingungen:

- *Kaufmodelle:* Förderbar sind alle direkten Kosten für den Erwerb von Hardware und Software, inklusive gegebenenfalls mit dem Erwerb direkt verbundene Service- und Wartungsgebühren bzw. Liefer- und Transportgebühren.
- *Gebührenmodelle (z.B. Miete, Leasing, Hosting, Flatrate):* Förderbar sind nur die im Förderungszeitraum angefallenen und bezahlten Kosten für Hardware und Software, inklusive gegebenenfalls mit der Nutzung direkt verbundene Service- und Wartungsgebühren.

3.5 Was ist hinsichtlich Projektlaufzeit zu beachten?

Der geplante **Projektstart** ist im eCall anzugeben. Der frühestmögliche Projektstart ist der Tag der Einreichung des Förderungsansuchens.

Projekte, die im Einreichzeitraum 1 (16.10.2023 – 15.01.2024 bis 12:00 Uhr) eingereicht werden, müssen bis **spätestens 01.04.2024** starten.

Projekte, die im Einreichzeitraum 2 (15.01.2024 ab 12:00 Uhr – 15.04.2024 bis 12:00 Uhr) eingereicht werden, müssen bis **spätestens 01.06.2024** starten.

Der Förderungszeitraum beträgt **12 Monate** ab Projektstart. Innerhalb des Förderungszeitraums müssen alle geförderten Leistungen umgesetzt sein.

Der Förderungszeitraum kann nicht verlängert werden.

3.6 Information und Beratung zu NIS2

Prüfen Sie vor Antragstellung, ob Ihr Unternehmen in den Anwendungsbereich der NIS2-Richtlinie fällt und welche Anforderungen sich für Ihr Unternehmen daraus ergeben. Konsultieren Sie gegebenenfalls zuständige Stellen oder zertifizierte IT-

Expertinnen bzw. IT-Experten, um eine fundierte Entscheidung vor Ihrer Antragstellung zu treffen.

Bei Fragen zu NIS bzw. NIS2 stehen weiterführende Informationen auf der Webseite der Anlaufstelle Netz- und Informationssystemsicherheitsgesetz (NISG) zur Verfügung. Eine Orientierungshilfe, ob ein Unternehmen von NIS2 betroffen sein könnte, bietet zusätzlich der Online-Ratgeber der WKÖ. Begriffsdefinitionen zu NIS2 inklusive detaillierte Beschreibungen zum Anwendungsbereich und den Anforderungen der NIS2-Richtlinie finden Sie direkt in der NIS2-Richtlinie.

Wir weisen darauf hin, dass die FFG keine Gewähr für die von Dritten zur Verfügung gestellten Informationen übernehmen kann.

4 DIE EINREICHUNG

4.1 Wie verläuft die Einreichung?

Die Einreichung ist nur elektronisch, innerhalb eines der beiden in Tabelle 1 definierten Einreichzeiträume, via **eCall** möglich, wobei der Einreichschluss spätestens mit dem Ende des zweiten Einreichzeitraums eintritt.

Alle Eingaben erfolgen mit dem elektronischen Antrag im eCall.

Wie funktioniert die Einreichung?

- **Registrierung**/Einloggen im eCall
- **Förderungsansuchen** anlegen und elektronischen Antrag direkt im eCall ausfüllen (Deutsch)
- **Zuordnung** des Unternehmens in den Anwendungsbereich der NIS2-Richtlinie in Form einer **Selbstdeklaration** im eCall
- **Darstellung des Umsetzungsplans** zur technischen Sicherheitsmaßnahme, die im Rahmen des geförderten Projekts umgesetzt werden soll (Beschreibung der Technologien bzw. Beratungsleistungen, Beschreibung des Zwecks, Zeitplan für die Umsetzung, erwarteter Effekt für das Unternehmen betreffend NIS2 Anforderungen)
- Angabe und Beschreibung der **Kosten**
- Förderungsansuchen abschließen und „Einreichung abschicken“ drücken

Nach erfolgreicher Einreichung wird automatisch eine Einreichbestätigung per eMail versendet. Sobald ein Förderungsansuchen eingereicht wurde, ist eine weitere Bearbeitung nicht mehr möglich.

Eingereicht wird durch die antragstellende Organisation oder durch vertretungsbefugte Personen. Eine Vertretungsbefugnis muss in schriftlicher Form vorliegen und ggf. auf Anfrage der FFG vorgelegt werden. Die FFG kann einen Nachweis für die Vertretungsbefugnis anfordern. Wenn Sie den Nachweis nicht bringen, behält sich die FFG das Recht vor, das Förderungsansuchen aus formalen Gründen abzulehnen.

Detaillierte Informationen finden Sie im eCall-Tutorial.

4.2 Wie dürfen vertrauliche Projektdaten verwendet werden?

Die FFG verarbeitet personenbezogene Daten der Förderungswerbenden und Förderungsnehmenden, die von den Betroffenen im Zuge des Förderungsansuchens bereitgestellt wurden, und von der FFG selbst erhobene Daten im Rahmen der Ausstellung der Förderungszusage und der Abwicklung des Vertragsverhältnisses, sowie im Wege der Transparenzportalabfrage generierte Daten gemäß § 32 Abs 5 TDBG 2012 zu nachstehenden Zwecken:

- Zur Behandlung des Förderungsansuchens und Beurteilung des Vorliegens der allgemeinen und speziellen Förderungsvoraussetzungen,
- Zum Zustandekommen der Förderungszusage und zur Abwicklung des Vertragsverhältnisses, insbesondere zur Verwaltung der Förderungsleistungen und der Kontrolle der Nachweise der Förderungsvoraussetzungen,
- Zur Erfüllung rechtlicher Verpflichtungen, insbesondere Meldepflichten und Kontrollzwecke zur Vermeidung von Doppelförderungen, und zwar § 38 iVm 18, 27, ARR, sowie § 12 FTFG und § 9 FFG-G.

Rechtsgrundlage der Verarbeitung ist daher zum einen Art 6 Abs 1 lit b DSGVO und daher die Notwendigkeit zur Erfüllung eines Vertragsverhältnisses und zum anderen Art 6 Abs 1 lit c DSGVO und daher die Erfüllung von rechtlichen Verpflichtungen.

Die personenbezogenen Daten werden in Erfüllung gesetzlicher Pflichten weitergegeben an:

- die Ministerien als Eigentümer:innen der FFG, weitere auftraggebende Stellen für die Abwicklung von Förderungsmaßnahmen (z.B. andere Ministerien, Bundesländer, KLIEN)
- an Dritte, das können sein: der Rechnungshof, Organe der EU, andere Bundes- oder Landesförderungsstellen.

Darüber hinaus kann es dazu kommen, dass Daten an das Bundeskanzleramt der Republik Österreich oder, in Erfüllung gesetzlicher Pflichten, an weitere Organe und Beauftragte des Bundes (Landes), des Rechnungshofes und der Europäischen Union übermittelt oder offengelegt werden müssen.

Projektinhalte und -ergebnisse können nur – soweit nicht eine rechtliche Verpflichtung der FFG besteht – mit Einwilligung der Förderungsnehmenden (Art 6

Abs 1 lit a DSGVO) veröffentlicht werden (z.B. auf der Website oder in Social Media Foren).

Auch für jede sonstige über diese Bestimmung hinausgehende Datenverarbeitung ist von der FFG eine Einwilligung der Betroffenen einzuholen.

Die FFG ist zur Geheimhaltung von Firmen- und Projektinformationen gesetzlich verpflichtet – nach § 9 Abs 4 Österreichische Forschungsförderungsgesellschaft mbH-Errichtungsgesetz, BGBl. I Nr. 73/2004.

Die FFG wird zur Sicherstellung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme technische und organisatorische Maßnahmen im Sinne des Art 32 DSGVO treffen, die ausreichend und geeignet sind, den Schutz der Daten vor zufälliger oder unrechtmäßiger Zerstörung, vor Verlust und vor Zugriff durch Unbefugte zu gewährleisten.

Weiterführende Informationen zur Wahrung der Vertraulichkeit und Sicherheit von personenbezogenen Daten während der Projektlaufzeit stehen im eCall-Tutorial.

5 DIE BEWERTUNG UND DIE ENTSCHEIDUNG

5.1 Wie erfolgen die Bewertung und die Entscheidung?

Die Entscheidung über eine Förderung erfolgt in einem **vereinfachten Bewertungsverfahren** jeweils nach Ende des in Tabelle 1 definierten Einreichzeitraums. Alle Anträge, die innerhalb des definierten Einreichzeitraums in der FFG eingereicht werden, werden im jeweiligen Bewertungsverfahren berücksichtigt. Die Auswahl erfolgt NICHT nach dem Prinzip „First Come, First Served“.

Werden innerhalb eines definierten Einreichzeitraums mehr Förderungsansuchen eingereicht als Budgetmittel zur Verfügung stehen, erfolgt die Auswahl der Förderungsansuchen, die geprüft werden, in zufälliger Reihenfolge mittels **Ziehungsverfahren per Zufallsprinzip**. Die Anzahl der gezogenen Anträge entspricht dabei den zur Verfügung stehenden Budgetmitteln.

Die gezogenen Förderungsansuchen werden durch die FFG auf Erfüllung der im Punkt 5.2 genannten Kriterien geprüft und entsprechend genehmigt oder abgelehnt.

- Im Fall einer **positiven Förderungsentscheidung** erhalten die Förderwerbenden eine Förderungszusage per eCall.
- Sollte eine **inhaltliche Überarbeitung** des Antrags notwendig sein, werden die Förderwerbenden davon in Kenntnis gesetzt und können die Mängel innerhalb einer von der FFG kommunizierten Frist **einmal** beheben. Erfolgt innerhalb dieser Frist keine Mängelbehebung, wird das Förderungsansuchen aus dem Verfahren ausgeschieden und der Grund im Ablehnungsschreiben erläutert.
- Ist die einreichende Organisation lt. Leitfaden nicht antragsberechtigt oder werden die im Punkt 5.2 genannten Kriterien nicht erfüllt, wird das Förderungsansuchen abgelehnt. Im Ablehnungsschreiben wird der Grund der **Ablehnung** per eCall erläutert.

Förderungsansuchen, die nicht gezogen und aus budgetären Gründen abgelehnt werden müssen, erhalten ein Ablehnungsschreiben per eCall.

Die Geschäftsführung der FFG trifft die **Förderungsentscheidung** auf Basis der FFG-Bewertung.

Bitte beachten Sie folgende wichtige Ergänzung (15.01.2024):

- Aufgrund ausreichend verfügbarer Förderungsmittel konnten alle im Einreichzeitraum 1 eingegangenen Förderungsansuchen gezogen werden. Diese Anträge unterliegen einer Prüfung durch die FFG gemäß den in Abschnitt 5.2 aufgeführten Kriterien und werden entsprechend genehmigt oder abgelehnt.
- Zusätzlich wurde die Ausschreibung zur Vergabe der verbleibenden Budgetmittel verlängert (Einreichzeitraum 2). Werden innerhalb des Einreichzeitraums 2 mehr Förderungsansuchen eingereicht als verbleibende Budgetmittel zur Verfügung stehen, erfolgt die Auswahl der Förderungsansuchen aus dem Einreichzeitraum 2 gemäß dem oben dargestellten Ziehungsverfahren per Zufallsprinzip.
- Unternehmen, die bereits ein Förderungsansuchen in Einreichzeitraum 1 eingereicht und eine Förderungszusage erhalten haben, können im Bewertungsverfahren zum Einreichzeitraum 2 nicht berücksichtigt werden.

5.2 Nach welchen Kriterien werden Förderungsansuchen bewertet?

Für eine positive Beurteilung sind alle Kriterien zu erfüllen.

Formale Kriterien:

- Ist der/die Förderungswerbende berechtigt, einen Antrag einzureichen (siehe Kapitel 3.2)?
- Sind die Angaben im Antrag ausreichend befüllt und wurde die richtige Sprache verwendet?

Inhaltliche Kriterien:

- **Welche Sicherheitsmaßnahmen sind geplant?**
  Die geplanten technischen Sicherheitsmaßnahmen inklusive Technologien und Beratungsleistungen sind nachvollziehbar beschrieben und entsprechen den Anforderungen der Ausschreibung.
- **Kosten – Welche Kosten zu Technologien und Beratungsleistungen fallen an?**
  Zweck und Inhalt der geplanten Kosten sind nachvollziehbar beschrieben, für die Erreichung der Projektziele relevant und förderbar.

6 DER ABLAUF DER FÖRDERUNG

6.1 Der Cyber Security Scheck in 5 Schritten

Abbildung 1 beschreibt den Ablauf der Fördermaßnahme von der Antragstellung bis zur Auszahlung der Förderung bei Förderungszusage.

Abbildung 1: Cyber Security Scheck in 5 Schritten

6.2 Welche Berichte und Abrechnungen sind erforderlich?

Nach Abschluss des Projekts und Zahlung aller Rechnungen zugekaufter Leistungen ist ein **Endbericht im eCall** zu legen. Die Endberichtlegung muss **spätestens einen Monat nach Projektende** erfolgen.

Der Endbericht umfasst:

- Bestätigung der vollständigen Umsetzung der Maßnahmen gemäß Antrag
- Falls relevant: Beschreiben Sie Abweichungen vom Förderungsansuchen, die sich bei der Umsetzung ergeben haben, insbes. betreffend Sicherheitsmaßnahmen, Technologien, Beratungsleistungen und Kosten (inkl. plausible Begründung der Abweichungen)
- Angabe und Beschreibung der Kosten

Sollte Ihr Projekt für eine **Stichprobenprüfung** ausgewählt worden sein, müssen die Rechnung(en) und Zahlungsbelege zu Technologien sowie zu Beratungsleistungen hochgeladen werden. Bitte beachten Sie, dass weitere Belege im Rahmen der Stichprobenprüfung nachgefordert werden können.

Die FFG behält sich vor, dass jedes geförderte Projekt im Rahmen der Stichprobenprüfung geprüft werden kann.

Beachten Sie hinsichtlich der Rechnungslegung:

- Auf der Rechnung muss die Technologie bzw. Beratungsleistung ersichtlich sein.
- Das Rechnungsdatum darf frühestens das Datum der Einreichung (im eCall) sein.
- Die Rechnung muss auf das einreichende Unternehmen ausgestellt sein.
- Die Rechnung muss vor dem Endbericht beglichen sein.

Auf Verlagen der FFG müssen Sie nachweisen können, dass alle abgerechneten Leistungen **im Förderungszeitraum erbracht** wurden.

Darüber hinaus können Organe des Bundes und der Europäischen Union Einsicht in die Bücher und Belege verlangen.

Unterstützung der Öffentlichkeitsarbeit: Die Förderungsnehmenden verpflichten sich bei Bedarf mit der FFG und den zuständigen Ressorts zur Unterstützung der Öffentlichkeitsarbeit zusammenzuarbeiten. Dies betrifft insbesondere die Bereitstellung von nicht vertraulichen Projektinformationen und Bildmaterial für elektronische Disseminationsportale und andere mediale Zwecke.

6.3 Wie erfolgt die Auszahlung der Förderung?

Die Auszahlung der Förderung erfolgt nach positiver Endberichtsprüfung.

War die Endberichtsprüfung positiv, wird die widmungsgemäße Verwendung der Förderungsmittel bestätigt (Kosten- und Förderungsanerkennungsschreiben) und die Förderung ausbezahlt. Eine Kürzung der Förderungsmittel aus inhaltlichen sowie formalen und rechtlichen Gründen ist möglich.

Die Originalbelege (z.B. Rechnung) und die dazugehörige Dokumentation des Zahlungsflusses (z.B. Kontoauszug) müssen 10 Jahre lang aufbewahrt und auf Verlangen der FFG übermittelt werden.

Die FFG hat während der gesamten Laufzeit der Förderung und auch danach die Möglichkeit, die von den Förderungsnehmenden gemachten Angaben und die Abwicklung der Förderung auf ihre Rechtmäßigkeit und Richtigkeit zu prüfen.

Bitte beachten Sie die Vorgaben für die Einstellung und Rückzahlung der Förderung in der FFG-Offensiv-Richtlinie.

6.4 Wie müssen Änderungen kommuniziert werden?

Folgende Änderungen müssen der FFG via eCall zur Überprüfung kommuniziert werden:

- Gesellschaftsrechtliche Änderungen
- Insolvenzverfahren
- Änderung des Firmenstandorts
- bei Verdacht eines Interessenkonfliktes, Betruges und/oder einer Korruption

7 RECHTSGRUNDLAGEN

Die Ausschreibung basiert auf der Richtlinie für die Österreichische Forschungsförderungsgesellschaft mbH zur Förderung von Forschung, Technologie, Entwicklung und Innovation für eine offensive themenoffene FTI-Förderung- (FFG-Offensiv-Richtlinie[2]).

Die europarechtliche Rechtsgrundlage ist die Richtlinie zu De-minimis-Beihilfen (Verordnung (EU) Nr. 1407/2013 der Kommission vom 18. Dezember 2013 über die Anwendung der Artikel 107 und 108 des Vertrags über die Arbeitsweise der Europäischen Union auf De-minimis-Beihilfen, ABL. L 352/1 vom 24.12.2013, verlängert durch die Verordnung (EU) 2020/972 der Kommission vom 2. Juli 2020).

[2] Richtlinie für die Österreichische Forschungsförderungsgesellschaft mbH zur Förderung von Forschung, Technologie, Entwicklung und Innovation für eine offensive themenoffene FTI- Förderung (FFG-Offensiv-Richtlinie) der Bundesministerin für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie und der Bundesministerin für Digitalisierung und Wirtschaftsstandort (GZ BMK 2021-0.891.331) (GZ BMDW 2021-0.900.577)

Bezüglich der Unternehmensgröße ist die jeweils geltende KMU-Definition[3] gemäß EU-Wettbewerbsrecht ausschlaggebend. Hilfestellung zur Einstufung finden sie auf der KMU-Seite der FFG.

Bezüglich der Anforderungen zu NIS2 und der Zuordenbarkeit von Unternehmen in den Anwendungsbereich der NIS2-Richtlinie ist die NIS2-Richtlinie[4] ausschlaggebend.

Sämtliche EU-Vorschriften sind in der jeweils geltenden Fassung anzuwenden.

8 WEITERE FÖRDERUNGSMÖGLICHKEITEN DER FFG

Sie interessieren sich für andere Förderungsmöglichkeiten der FFG?

Das **Förderservice** ist die zentrale Anlaufstelle für Ihre Anfragen zu den Förderungen und Beratungsangeboten der FFG. Kontaktieren Sie uns, wir beraten Sie gerne!

Kontakt: FFG-Förderservice, T: +43 (0) 57755-0, E: foerderservice@ffg.at

Web: https://www.ffg.at/foerderservice

Beachten Sie die Förderung Skills Schecks 2023. Skills Schecks unterstützen Unternehmen mit Niederlassung in Österreich beim Kompetenzaufbau ihrer Mitarbeiter:innen. Gefördert werden externe Weiterbildungskosten.

Weitere Förderungsmöglichkeiten der FFG finden Sie hier, unter anderem auch Förderungen speziell in den Schwerpunkten Digitalisierung sowie Menschen, Qualifikation und Gender.

Weitere nationale und europäische Fördermöglichkeiten im Bereich der Cybersicherheit finden Sie auf der Förderübersicht des Nationalen Koordinierungszentrums für Cybersicherheit (NCC-AT).

[3] Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, ABl. L 124 vom 20. Mai 2003.

[4] RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)