Informationssicherheit
Statistik Austria

Impressum

Herausgeber: Bundesanstalt Statistik Österreich (Statistik Austria)
Verantwortung für fachliche Inhalte: Generaldirektion
Redaktionelle Verantwortung: IT-Abteilung

Gültig ab: 24.5.2022
Gültig bis: Revision

Inhaltsverzeichnis

1 Informationssicherheit

Für die Bundesanstalt Statistik Österreich (im Folgenden Statistik Austria) stellt die Sicherheit und der Schutz der von ihr gesammelten, verarbeiteten und verwalteten Daten sowie Informationen eine vordringliche Aufgabe dar.

Informationssicherheit (InSi) umfasst den Schutz von Daten und Informationen mit einem identifizierten Schutzbedarf vor Verlust, Manipulation und unerwünschter Offenlegung und damit auch den Schutz der entsprechenden Daten- und Informationsträger und Einrichtungen zur Daten- und Informationsverarbeitung. Auch Informationen auf Papier, digitale Datenträger und die verbale Informationsübertragung sind Gegenstand der Informationssicherheit.

Das vorliegende Dokument beinhaltet die Ziele und Führungsgrundsätze von Statistik Austria zum Thema Informationssicherheit sowie die Anforderungen an ein InSi-Managementsystem (siehe Abschnitt 3.2), durch das ein angemessenes InSi-Niveau sichergestellt werden soll. Dieses basiert auf der international anerkannten Norm ISO 27001, wurde von der Generaldirektion von Statistik Austria in Kraft gesetzt und wird in einem jährlichen Zyklus auf Aktualität überprüft und bei Änderung durch diese freigegeben.

Die IT-Abteilung wurde mit der Einrichtung und kontinuierlichen Weiterentwicklung eines InSi-Managementsystems beauftragt. Damit verbunden ist die Etablierung der Rolle einer bzw. eines InSi-Beauftragten, worüber die übergeordnete Koordination, die Steuerung und das Berichtswesen für dieses Managementsystem wahrgenommen werden.

Das InSi-Team stellt themenspezifische Richtlinien zur Verfügung und überprüft regelmäßig ihre Aktualität. Änderungen der Richtlinien sind von der Generaldirektion zu genehmigen. Alle für die Informationssicherheit relevanten Dokumente sind im Intranet von Statistik Austria verfügbar.

Eine Gruppe von Informationen mit besonders hohem Schutzbedarf bilden „personenbezogene Daten“, deren Informationssicherheit nach den Vorgaben der europäischen Datenschutz-Grundverordnung (DSGVO) und des Datenschutzgesetzes (DSG) sicherzustellen ist. Die bzw. der für dieses Thema im Organisationsbereich Zentrale Dienste etablierte Datenschutzbeauftragte und die bzw. der InSi-Beauftragte arbeiten als Mitglieder des InSi-Teams eng zusammen.

Regelmäßige Überprüfungen sowie die laufende Überwachung der InSi-Prozesse, der Einhaltung der Richtlinien und der implementierten Sicherheitsmaßnahmen geben Aufschluss über deren Wirksamkeit und bilden die Grundlage für notwendige Änderungen und die kontinuierliche Verbesserung. Die Wirksamkeit des InSi-Managementsystems insgesamt wird regelmäßig von der Generaldirektion bewertet, um dessen fortdauernde Eignung und Angemessenheit sicherzustellen.

Bei der Umsetzung und kontinuierlichen Weiterentwicklung des InSi-Managementprozesses (siehe Abbildung 2) ist auf Effektivität und Effizienz vor allem aber auf die Balance zwischen der nötigen Informationssicherheit und der Aufrechterhaltung der ungestörten Abläufe des Betriebes zu achten.

Die Generaldirektion

2 Informationssicherheitsziele

Im Rahmen der Informationssicherheit sind allgemeine und themenspezifische Schutzziele festgelegt.

2.1 Allgemeine Schutzziele

Die folgenden zentralen Schutzziele der Informationssicherheit stellen die oberste Ebene der Sicherheitsanforderungen für die von Statistik Austria gesammelten, verarbeiteten und verwalteten Daten und Informationen dar:

- **Vertraulichkeit**
  Statistik Austria stellt jederzeit sicher, dass ihre schutzbedürftigen Daten und Informationen nur berechtigten Benutzerinnen bzw. Benutzern zur Kenntnis gelangen bzw. von diesen eingesehen und verarbeitet werden. Das gilt für Personen und sinngemäß auch für Systeme. Dabei werden im Besonderen die gesetzlichen Anforderungen für den Datenschutz und die Erstellung und Veröffentlichung von Statistiken berücksichtigt.

- **Integrität**
  Es wird sichergestellt, dass die Daten und Informationen nicht unautorisiert oder unbemerkt verändert oder manipuliert werden. Das gilt insbesondere für die technische Verarbeitung und Übermittlung von Daten. Bei den dabei eingesetzten Sicherheitsmechanismen wird auf hohe Widerstandsfähigkeit geachtet.

- **Verfügbarkeit**
  Es wird sichergestellt, dass die Daten und Informationen im Rahmen der getroffenen Vereinbarungen den berechtigten Personen und Systemen zur Verfügung stehen, wenn sie benötigt werden. Die Betriebssicherheit der IT-Systeme und -Verfahren wird gewährleistet, Systemausfälle verhindert bzw. ihre Auswirkungen minimiert sowie die Daten vor Verlust geschützt. Bei den eingesetzten Sicherheitsmechanismen wird auf hohe Robustheit geachtet.

Neben diesen zentralen Schutzzielen sind folgende weitere Schutzziele definiert:

- **Authentizität**
  Die Urheberschaft und Unverfälschtheit der Daten und Informationen wird durch den Nachweis ihrer Authentizität sichergestellt. Damit wird ihre Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit gewährleistet.

- **Nachweisbarkeit**
  Die Nachweisbarkeit (Nichtabstreitbarkeit, Urheberschaft) von Handlungen, insbesondere Kommunikationshandlungen im Kontext der Informationsverarbeitung wird sichergestellt. Vollzogene Handlungen können so nicht unzulässig abgestritten werden.

- **Beweissicherung**
  Die Revisionsfähigkeit von sicherheitsrelevanten Systemen und Prozessen wird sichergestellt.

2.2 Themenspezifische Schutzziele

Zusätzlich sind themenspezifische Schutzziele bzw. Maßnahmen definiert, deren Erreichung bzw. Durchführung zur Gewährleistung und Aufrechterhaltung der Informationssicherheit notwendig sind. Diese Schutzziele stellen auch die Erklärung zur Anwendbarkeit der Maßnahmenziele aus dem Anhang A der Norm ISO/IEC 27001 (Statement of Applicability) dar. Es kommen alle Maßnahmenziele zur Anwendung.

2.2.1 Organisation der Informationssicherheit

1. Eine InSi-Organisation (siehe Abschnitt 3.3) ist in Statistik Austria eingerichtet.
2. Notwendige Rollen mit definierten Aufgaben und Verantwortlichkeiten sind in der InSi-Organisation festgelegt und Personen zugewiesen.
3. In Statistik Austria generell notwendige InSi-relevante Rollen mit definierten Aufgaben und Verantwortlichkeiten sind für Mitarbeiterinnen bzw. Mitarbeiter sowie externe Dienstleisterinnen und Dienstleister festgelegt und Personen zugewiesen.

2.2.2 Personalsicherheit

1. Vor Aufnahme der Beschäftigung ist sichergestellt, dass Beschäftigte ihre Verantwortlichkeiten in Bezug auf Informationssicherheit verstehen und der Rollen für die sie vorgesehenen sind, gerecht werden.
2. Während der Beschäftigung ist sichergestellt, dass Beschäftigte sich ihrer Verantwortlichkeiten in Bezug auf Informationssicherheit bewusst sind und diesen nachkommen.
3. Bei Beendigung bzw. Änderung der Beschäftigung ist sichergestellt, dass der Schutz der Interessen von Statistik Austria in Bezug auf Informationssicherheit sowie ihrer Daten und Informationen gewahrt bleibt.

Die Punkte 1. - 3. gelten sinngemäß auch für externe Dienstleisterinnen und Dienstleister und deren Beschäftigte.

2.2.3 Verwaltung von Informationssicherheitswerten

1. Der Begriff „Informationssicherheitswerte“ umfasst
    - Daten und Informationen,
    - Daten- und Informationsträger und
    - Einrichtungen zur Daten- und Informationsverarbeitung,

    jeweils mit Schutzbedarf und im Zuständigkeitsbereich von Statistik Austria. Diese sind identifiziert und Verantwortlichkeiten zu ihrem Schutz festgelegt.
2. Die unerlaubte Offenlegung, Veränderung, Entfernung oder Zerstörung von Daten und Informationen, die auf Datenträgern gespeichert sind, wird unterbunden.

2.2.4 Klassifizierung von Daten und Informationen

1. Es ist sichergestellt, dass Daten und Informationen ein angemessenes Schutzniveau entsprechend ihrer Bedeutung für die Organisation erhalten.
2. Ein Schema zur Klassifizierung von Daten und Informationen ist definiert. Dieses enthält auch die Klassifizierung von personenbezogenen Daten. Daten und Informationen werden damit auf Basis des ermittelten Schutzbedarfs eingestuft.
3. Daten und Informationen werden gemäß den Vorgaben für die jeweils getroffene Einstufung gekennzeichnet und zu ihrem Schutz gehandhabt.
4. Insbesondere die Handhabung und der Schutz von personenbezogenen Daten sowie die statistische Geheimhaltung in Publikationen und bei der Weitergabe von Daten und Informationen sind entsprechend den gesetzlichen Anforderungen sichergestellt.

2.2.5 Zugangssteuerung

1. Der Zugang zu Daten und Informationen sowie zu Einrichtungen zur Daten- und Informationsverarbeitung ist eingeschränkt, sowohl physisch als auch logisch.
2. Es ist sichergestellt, dass nur befugte Benutzerinnen bzw. Benutzer Zugang zu Systemen, Diensten und Anwendungen erhalten und unbefugter Zugang unterbunden wird.
3. Benutzerinnen bzw. Benutzer sind für den Schutz ihrer Authentisierungsinformation verantwortlich.

2.2.6 Physische und umgebungsbezogene Sicherheit

1. Sicherheitsperimeter und -zonen sind definiert und unbefugter Zutritt wird verhindert.
2. Physische Beschädigung oder Beeinträchtigung durch umweltbedingte Bedrohungen oder technisches Versagen, Verlust, Diebstahl sowie vorsätzliche oder fahrlässige Gefährdung von Daten und Informationen sowie Einrichtungen zur Daten- und Informationsverarbeitung wird verhindert.
3. Die sichere Wiederverwendung oder Entsorgung von Geräten und Betriebsmitteln zur Informationsverarbeitung ist gewährleistet.

2.2.7 Betriebssicherheit

1. Der ordnungsgemäße und sichere Betrieb sowie die Integrität von Einrichtungen zur Daten- und Informationsverarbeitung sind sichergestellt.
2. Daten und Informationen sowie Einrichtungen zur Daten- und Informationsverarbeitung sind vor Schadsoftware geschützt.
3. Die Ausnutzung technischer Schwachstellen wird verhindert.
4. Daten und Informationen sind vor Verlust geschützt.
5. Ereignisse mit Bezug zur Informationssicherheit werden aufgezeichnet und entsprechende Nachweise werden erzeugt.

6. Die Auswirkung von Überprüfungstätigkeiten auf Systeme im Betrieb wird minimiert.

2.2.8 Kryptographische Maßnahmen

1. Der angemessene und wirksame Gebrauch von Kryptographie zum Schutz der Vertraulichkeit, Authentizität und Integrität von Daten und Informationen ist sichergestellt.

2.2.9 Netzwerksicherheitsmanagement

1. Der Schutz von Daten und Informationen in Netzwerken und den diese unterstützenden Einrichtungen zur Daten- und Informationsverarbeitung ist sichergestellt.

2.2.10 Informationsübertragung

1. Die Sicherheit von Daten und Informationen bei deren Übertragung wird aufrechterhalten, sowohl innerhalb Statistik Austria als auch beim Austausch mit externen Stellen.

2.2.11 Softwaretechnik, Anschaffung und Instandhaltung von IKT-Systemen

1. Informationssicherheit ist ein fester Bestandteil über den gesamten Lebenszyklus von Informations- und Kommunikationstechniksystemen (IKT-Systemen). Das beinhaltet auch die Anforderungen an IKT-Systeme, die Dienste über öffentliche Netze bereitstellen.
2. Informationssicherheit ist im Softwaretechnikprozess von IKT-Systemen geplant und umgesetzt.
3. Der Schutz von Daten und Informationen, die für das Testen verwendet werden, ist sichergestellt.

2.2.12 Dienstleister- und Lieferantenbeziehungen

1. Für Dienstleisterinnen und Dienstleister als auch für Lieferantinnen und Lieferanten zugängliche Daten und Informationen sowie Einrichtungen zur Daten- und Informationsverarbeitung sind angemessen geschützt.
2. Vereinbarungen zur Informationssicherheit sind mit den Dienstleisterinnen und Dienstleistern sowie Lieferantinnen und Lieferanten getroffen.
3. Die Einhaltung der Informationssicherheit im Zuge der Dienstleistungserbringung und Lieferung wird angemessen überwacht und überprüft.

2.2.13 Handhabung von Informationssicherheitsvorfällen

1. Eine konsistente und wirksame Herangehensweise für die Handhabung von Informationssicherheitsvorfällen sowie Risiken in Bezug auf Informationssicherheit ist sichergestellt.

2.2.14 Informationssicherheitsaspekte im Zuge des Betriebskontinuitätsmanagement

1. Betriebskontinuitätsmanagement (auch Business Continuity Management, BCM), das die Aufrechterhaltung bzw. schnelle Wiederaufnahme von kritischen Geschäftsprozessen bei Notfällen oder Krisen zum Ziel hat, ist sichergestellt.
2. Für kritische Einrichtungen zur Daten- und Informationsverarbeitung stehen vorsorglich auf Basis von Business Impact Analysen erstellte Notfall- und Wiederherstellungspläne zur Ver-

fügung. Diese kommen in entsprechenden Notfall-, Katastrophen- und Krisensituationen zur Anwendung.

3. Die Aktualität und kontinuierliche Verbesserung des Betriebskontinuitätsmanagements ist durch die regelmäßige Überprüfung der vorsorglich erstellten Notfall- und Wiederherstellungspläne sowie durch die Durchführung von regelmäßigen Übungen sichergestellt.
4. Die Verfügbarkeit von Einrichtungen zur Daten- und Informationsverarbeitung mit Hilfe angemessener Redundanzen ist sichergestellt.

2.2.15 Compliance

1. Verstöße gegen gesetzliche, regulatorische, vertragliche oder selbstauferlegte Verpflichtungen mit Bezug zur Informationssicherheit und gegen bestehende Sicherheitsanforderungen werden vermieden.
2. Informationssicherheit ist in Übereinstimmung mit den in Statistik Austria geltenden Richtlinien für Informationssicherheit umgesetzt und wird entsprechend gewährleistet.

3 Umsetzung der Informationssicherheit

Die Umsetzung der Informationssicherheit erfolgt über ein InSi-Managementsystem, das nach den Anforderungen des internationalen Standards ISO 27001 betrieben und auf alle Standorte, Organisationseinheiten, Geschäftsprozesse, Verarbeitungen, Produkte und Leistungen von Statistik Austria angewendet wird. Darin werden Richtlinien und Maßnahmen festgelegt, die im Rahmen des InSi-Managementsystems gesteuert und kontinuierlich weiterentwickelt werden.

3.1 Informationssicherheitsarchitektur

Die InSi-Architektur legt die Hierarchie von Grundsätzen, Richtlinien und Maßnahmen fest – siehe Abbildung 1:

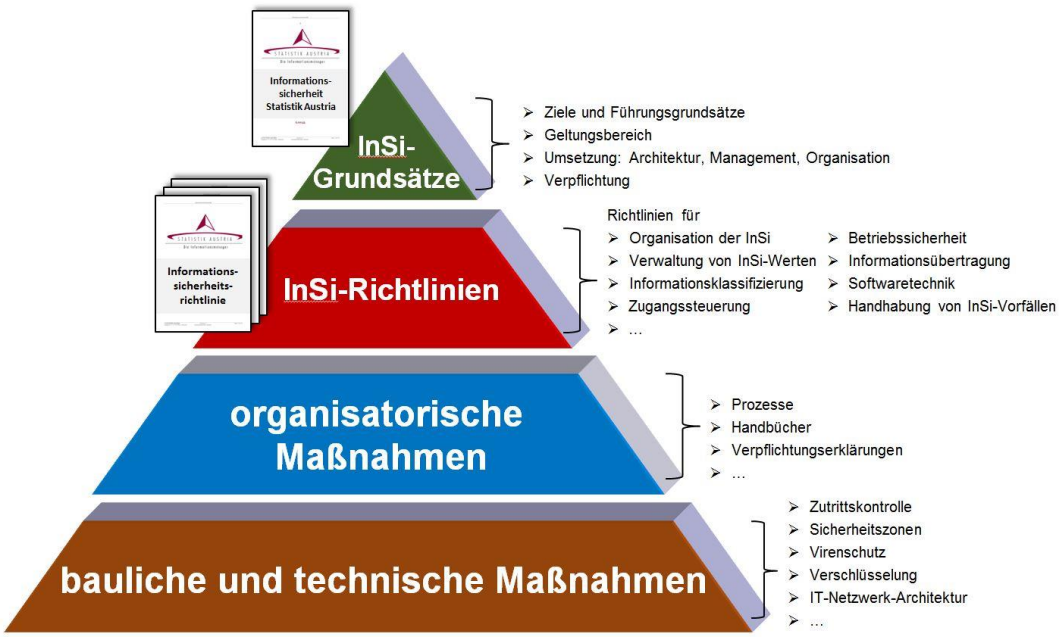

Abbildung 1: InSi-Architektur

Auf oberster Ebene der InSi-Architektur befinden sich die InSi-Grundsätze, durch die die Ziele und Führungsgrundsätze zum Thema Informationssicherheit festgelegt werden. Sie bilden den Rahmen für die darunterliegenden Richtlinien und Maßnahmen.

Die Richtlinien beschreiben themenspezifisch die grundlegenden Sicherheitsanforderungen auf Basis der definierten Schutzziele und werden bei Bedarf durch Maßnahmen umgesetzt. Diese Maßnahmen können organisatorischer, baulicher oder technischer Natur sein. Sie können – je nach Anforderung – für Statistik Austria insgesamt oder für einzelne Bereiche oder Projekte festgelegt werden.

3.2 Informationssicherheitsmanagementsystem

Über das InSi-Managementsystem werden die Richtlinien und Maßnahmen der InSi-Architektur gesteuert, auf Angemessenheit und Wirksamkeit überprüft sowie kontinuierlich weiterentwickelt und verbessert. Abbildung 2 zeigt das Managementsystem als Prozess:

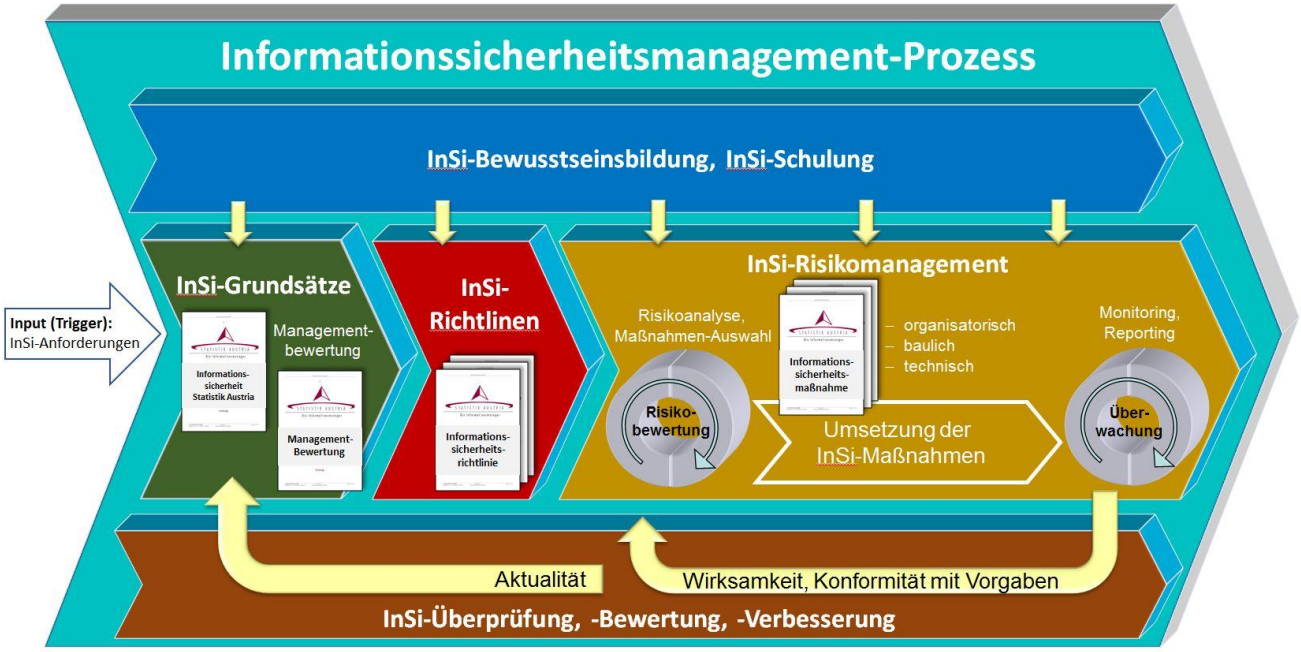

Abbildung 2: InSi-Managementprozess

Vorrangige Ziele sind die bestmögliche Erreichung der in Kapitel 2 festgelegten InSi-Ziele, die Identifizierung, Analyse und Bewertung der diesbezüglichen Risiken sowie die Herbeiführung erforderlicher Entscheidungen für notwendige Verbesserungen der Informationssicherheit durch die zuständigen Personen.

3.3 Informationssicherheitsorganisation

Die InSi-Organisation führt im Rahmen der Organisationsstruktur von Statistik Austria den InSi-Managementprozess durch und hat das Ziel, bei der praktischen Umsetzung der Informationssicherheit zu unterstützen und zu beraten. Sie besteht aus Personen, die zusätzlich zu ihrer Linientätigkeit Funktionen und Rollen der Informationssicherheit wahrnehmen.

3.4 Verpflichtung der Organisation

Die Generaldirektion sowie alle Mitarbeiterinnen bzw. Mitarbeiter bekennen sich zu den Zielen der Informationssicherheit und verpflichten sich zur Einhaltung der entsprechenden Richtlinien mit Bezug zur Informationssicherheit. Externe Dienstleisterinnen und Dienstleister werden ebenfalls zur Einhaltung verpflichtet.

Die Generaldirektion unterstützt die Führungskräfte bei der Planung, Durchführung und Kontrolle der erforderlichen Sicherheitsmaßnahmen, stellt die Einhaltung der Regelungen sicher und verfügt beim Auftreten von diesbezüglichen InSi-Risiken angemessene Maßnahmen und Sanktionen.

3.5 Informationen im Intranet von Statistik Austria

Alle in Statistik Austria geltenden Richtlinien zur Informationssicherheit sowie weitere Informationen und Dokumente zu diesem Thema sind im Intranet von Statistik Austria verfügbar.

4 Abbildungsverzeichnis

5 Dokumentmanagement

Die jährlich stattfindende Überprüfung des Dokuments durch die InSi-Organisation und die Generaldirektion werden in den entsprechenden Sitzungsprotokollen dokumentiert. Wird das Dokument aufgrund der Überprüfung oder anderer Anlässe geändert, wird eine neue Version erstellt, diese durch die Generaldirektion genehmigt und freigegeben und den Mitarbeiterinnen bzw. Mitarbeitern von Statistik Austria zur Kenntnis gebracht.

Datum	Version	Beschreibung	verantwortlich
2018-09-20	00.98	Erstellung des Entwurfs	Christian Brandner
2018-10-23	01.00	Erstellung der Version 01.00 nach Überprüfung durch das Management	Christian Brandner
2019-02-01	01.00	Genehmigung und Freigabe der Version 01.00 durch die Generaldirektion	Gabriela Petrovic Konrad Pesendorfer
2021-10-29	02.00	Genehmigung und Freigabe der Version 02.00 (Vermerk der Kenntnisnahme des Dokuments durch die neue Generaldirektion)	Gabriela Petrovic Tobias Thomas
2022-04-26	03.00	Erstellung der Version 03.00: Vermerk des Anwendungsbereichs des InSi-Managementsystems (Statement of Applicability)	Christian Brandner
2022-05-25	03.00	Genehmigung und Freigabe der Version 03.00 durch die Generaldirektion	Gabriela Petrovic Tobias Thomas