COMMITTEE OF MINISTERS
COMITÉ DES MINISTRES

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

MINISTERS' DEPUTIES
DÉLÉGUÉS DES MINISTRES

CM Documents
Documents CM

CM(2022)10-final

09/02/2022

European Committee on Democracy and Governance (CDDG)

Committee of Ministers' Guidelines on the use of information and communication technology (ICT) in electoral processes in Council of Europe member States

Unofficial translation into German

Comité européen sur la démocratie et la gouvernance (CDDG)

Lignes directrices du Comité des Ministres sur l'utilisation des technologies de l'information et de la communication (TIC) dans les processus électoraux des États membres du Conseil de l'Europe

Traduction non-officielle en allemand

Europäischer Ausschuss für Demokratie und Governance (CDDG)

Leitlinien des Ministerkomitees zum Einsatz von Informations- und Kommunikationstechnologien (IKT) bei Wahlen in den Mitgliedstaaten des Europarats

MINISTERSTELLVERTRETER Dokumente des Ministerkomitees (CM) **CM(2022)10-endg** 9. Februar 2022

1424. Sitzung, 9. Februar 2022

2 Aktuelle politische Fragen

2.4 Europäischer Ausschuss für Demokratie und Governance (CDDG)

b. Leitlinien des Ministerkomitees zum Einsatz von Informations- und Kommunikationstechnologien (IKT) bei Wahlen in den Mitgliedstaaten des Europarats

---

Leitlinien des Ministerkomitees zum Einsatz von Informations- und Kommunikationstechnologien (IKT) bei Wahlen in den Mitgliedstaaten des Europarats

Einleitung

Freie und faire Wahlen und Referenden gehören zu den Grundpfeilern der Demokratie. Die Integrität des Wahlprozesses ist für das Vertrauen der Öffentlichkeit in die Legitimität demokratischer Institutionen grundlegend.

Derzeit lässt sich beobachten, dass in allen Lebensbereichen zunehmend auf Informations- und Kommunikationstechnologien (IKT) zurückgegriffen wird, so auch in Verwaltungsangelegenheiten im Zusammenhang mit Wahlen. Mit diesen Leitlinien soll zur Wahrung der Integrität von Wahlprozessen und damit auch zur Förderung des Vertrauens der Bürger in die Demokratie beigetragen werden. Die Leitlinien formulieren Anforderungen und Sicherheitsvorkehrungen, die im Hinblick auf den Einsatz von IKT in den unterschiedlichen Phasen des Wahlprozesses in die Rechtsvorschriften der Mitgliedstaaten des Europarats aufgenommen werden sollten.

Anwendungsbereich der Leitlinien

Für den Umgang mit Daten und Prozessen im Zusammenhang mit Wahlen können Staaten z.B. auf folgende IKT-Lösungen zurückgreifen:

- Wählerverzeichnisse und Registrierung von Wählern, Beobachtern, der Medien usw.;
- Sammeln von elektronischen Unterschriften zu bestimmten Themen (z.B. Initiativen oder Petitionen), für Kandidaten oder Parteien;
- Veröffentlichung von Informationen im Zusammenhang mit Wahlen im Internet;
- elektronische Übertragung von Wahldaten zwischen kommunalen, regionalen und zentralen Wahlbehörden;
- Online-Schulungen von Wahlhelfern und anderen Beteiligten oder elektronische Akkreditierung von Beobachtern;
- Ermittlung, Verarbeitung, Übermittlung und Veröffentlichung von Wahlergebnissen;
- Beobachtung von verschiedenen Aktivitäten im Zusammenhang mit Wahlen, usw.

Des Weiteren wurden IKT-Lösungen im Kontext der Corona-Pandemie diskutiert, da die ordentliche Durchführung des Wahlprozesses beeinträchtigt war.

Elektronische Daten und Prozesse können beispielsweise durch verbesserte Barrierefreiheit, mehr Raum für Interaktion und erhöhte Transparenz die Ausübung politischer Rechte verbessern. Auch in Verwaltungsangelegenheiten im Zusammenhang mit Wahlen kann man im Hinblick auf Schnelligkeit, Effizienz und Genauigkeit hiervon profitieren. Gleichzeitig steigt mit der Umsetzung und dem Einsatz von IKT die Komplexität und ist man verstärkt den Bedrohungen und Risiken ausgesetzt, welche mit den eingesetzten IKT-Lösungen oder -Systemen verbunden sind.

Diese Leitlinien behandeln den Einsatz von IKT-Lösungen durch oder im Auftrag von zuständigen Wahlbehörden in allen Phasen des Wahlprozesses außer e-Voting und e-Counting, die in der Empfehlung CM/Rec(2017)5 zu Normen für e-Voting behandelt werden und somit über den Rahmen dieser Leitlinien hinausgehen. Diese Leitlinien gelten dagegen auch für hybride Auszählungsformen, bei denen einige IKT eingesetzt werden, die aber nicht unter die Definition von e-Voting gemäß CM/Rec(2017)5 fallen. Diese Leitlinien behandeln allerdings nicht den Einsatz von IKT im Zusammenhang mit Wahlprozessen durch Andere, insbesondere für Wahlkampfaktivitäten wie politischem Mikrotargeting durch politische Parteien oder für Informationen durch die Medien.

Grundprinzipien demokratischer Wahlen und Referenden

Der Einsatz von IKT sollte – ebenso wie die Nutzung aller anderen Technologien in Wahlprozessen – den Grundsätzen demokratischer Wahlen und Referenden und anderen relevanten Prinzipien entsprechen und mit anderen grundlegenden Erwägungen wie Sicherheit und Barrierefreiheit in Einklang gebracht werden.

Die Abhaltung demokratischer Wahlen und Referenden sollte in Übereinstimmung mit bestimmten Grundsätzen erfolgen, welche ihnen ihren demokratischen Status verleihen. Der 2002 von der Europäische Kommission für Demokratie durch Recht (Venedig-Kommission) angenommene Verhaltenskodex für Wahlen[1] dient dem Europarat in diesem Bereich als Referenzdokument. Er definiert die „Grundsätze des europäischen Wahlerbes“ unter zwei Aspekten: die verfassungsmäßigen Grundsätze des Wahlrechts und bestimmte grundlegende Bedingungen für deren Umsetzung.

Entsprechend dem Verhaltenskodex für Wahlen von 2002 kann die Bedeutung der wesentlichen Grundsätze und Bedingungen für Wahlen wie folgt zusammengefasst werden:

- „Allgemeines Wahlrecht“: Jeder Mensch ist unter bestimmten Bedingungen wie Alter, Staatsangehörigkeit oder Wohnsitz wahlberechtigt und wählbar;
- „Gleiches Wahlrecht“: Jeder Wähler hat die gleiche Stimmenzahl; jede Stimme hat das gleiche Gewicht und die Gleichheit der Chancen muss sichergestellt sein;
- „Freies Wahlrecht“: Der Wähler hat das Recht auf freie Willensbildung und -äußerung ohne Zwang oder unzulässige Einflussnahme;
- „Geheimes Wahlrecht“: Der Wähler hat das Recht auf geheime Wahl als Einzelperson, und der Staat hat die Pflicht, dieses Recht zu schützen;
- „Unmittelbares Wahlrecht“: Die vom Wähler abgegebenen Stimmen bestimmen unmittelbar den/die gewählte(n) Person(en);
- „Regelmäßigkeit der Wahlen“: Wahlen müssen in regelmäßigen Abständen stattfinden;
- „Wahrung der Grundrechte“: Demokratische Wahlen setzen die Achtung der Menschenrechte wie die Meinungsfreiheit, das Recht auf Freizügigkeit, die Versammlungs- und Vereinsfreiheit voraus;
- „Normebenen und Stabilität des Wahlrechts“: Die Bestimmungen des Wahlrechts müssen mindestens einen gesetzgebenden Rang besitzen; technische Regelungen und Detailregeln können in Verordnungen der Exekutive aufgenommen werden. Die Grundelemente des Wahlrechts sollten bis ein Jahr vor einer Wahl nicht mehr verändert werden oder müssten auf verfassungsrechtlicher Ebene oder auf einer Ebene, die über dem Parlamentsgesetz angeordnet ist, bearbeitet werden;
- „Verfahrensgarantien“: Sie beinhalten unter anderem Maßnahmen, die auf die Organisation der Wahlen durch ein neutrales Gremium, die Beobachtung der Wahlen durch nationale und internationale Beobachter wie auch das Vorhandensein eines wirksamen Beschwerdesystems abzielen;

Diese Leitlinien haben allgemeinen Charakter und sind für alle Formen eines Einsatzes von IKT in den betrachteten Phasen des Wahlprozesses gedacht. Bei demokratischen Wahlen und Referenden sollten neben den wesentlichen Grundsätzen für Wahlen und der Achtung der Grundrechte auch alle anderen einschlägigen rechtlichen Grundsätze eingehalten werden. Hierzu gehören die einschlägigen internationalen Verpflichtungen, Empfehlungen und Normen, insbesondere zu Wahlen und IKT, beispielsweise die, die in der Präambel der Empfehlung CM/Rec(2017)5 zu Normen für e-Voting aufgeführt werden. Einschlägige Rechtsgrundsätze finden sich darüber hinaus auf nationaler und subnationaler Ebene.

Die Sicherheit (der Daten und des Systems) sollte des Weiteren als einer der Leitgrundsätze betrachtet werden, der für die Konzeption, die Entwicklung und den Einsatz von IKT-Lösungen in allen Phasen des Wahlprozesses gilt und somit einen menschenzentrierten „Security by Design“-Ansatz sicherstellt. Sind beispielsweise die Integrität und Authentizität, die Verfügbarkeit und Zuverlässigkeit, die Geheimhaltung und Vertraulichkeit, die Gebrauchstauglichkeit und Barrierefreiheit gewährleistet, bedeutet dies, dass das System und die Informationen vor möglichen Risiken geschützt sind, die diese Ziele gefährden würden. Alle Risikobewertungen sollten daher an die jeweils betroffene Phase des Wahlzyklus angepasst sein. Ein wichtiger Teil der Sicherheitsbemühungen besteht darin, auf der Grundlage vorab festgelegter Kriterien für eine Risikoakzeptanz und vorab festgelegter Methoden ein kontinuierliches Risikomanagement durchzuführen. IKT-Lösungen sollten dem neuesten Stand der Technik entsprechen und auf geprüften Algorithmen und Konzepten aufbauen, die von weiten Teilen der Wissenschaft getragen werden. So kann das Vertrauen in den Prozess gestärkt werden.

Für die Regelung des Einsatzes von IKT-Lösungen im Wahlprozess wird aufgrund ihrer positiven Auswirkungen auf die Qualität der Regelungen eine Interdisziplinarität sehr anempfohlen. Die Leitlinien bauen darüber hinaus auf den im Rahmen der Nutzung von elektronischen Mitteln zur Abstimmung und Auszählung in den Mitgliedstaaten gesammelten Erfahrungen und auf Praxisbeispielen auf.

[1] Verhaltenskodex für Wahlen (CDL-AD(2002)023rev2-cor), angenommen von der Venedig-Kommission auf ihrer 52. Plenarsitzung (Venedig, 18.-19. Oktober 2002).

Allgemeine Leitlinien für alle Phasen des Wahlprozesses

In den folgenden Leitlinien bezieht sich der Begriff „Mitgliedstaat“ auf die für die Regulierung, Durchführung und Überwachung des betreffenden Wahlprozesses zuständige Stelle. Üblicherweise, wenn auch nicht immer, bezieht er sich auf die für die Durchführung von Wahlen zuständigen Stellen auf kommunaler, regionaler oder zentraler Ebene. Er kann sich auch auf andere öffentliche Einrichtungen wie – je nach Sachlage – das Parlament oder die Regierung beziehen.

1. Die Mitgliedstaaten sollten dafür sorgen, dass IKT-Lösungen die Grundsätze demokratischer Wahlen und Referenden einhalten und dass andere einschlägige Grundsätze hinreichend berücksichtigt werden.

Es sollten allgemeine rechtliche Grundsätze ausgearbeitet werden, die für die unterschiedlichen Phasen des Wahlprozesses Anwendung finden. Oft ist es nicht möglich – auch bei papierbasierten oder manuellen Lösungen – alle Grundsätze im selben Maße umzusetzen. Das kann zweierlei Gründe haben:

1. Es kann einen tatsächlichen oder empfundenen Konflikt zwischen Grundsätzen geben (z.B. zwischen Geheimhaltung und Datenschutz einerseits und Transparenz andererseits), bei dem ein Gleichgewicht dafür definiert werden muss, in welchem Maße sie jeweils sichergestellt sein müssen.
2. Üblicherweise beruhen Lösungen – ob in Papierform und manuell oder IKT – auf Annahmen (z.B. zur Interaktion der Nutzer mit der IKT oder untereinander oder über die Fähigkeiten möglicher Angreifer). Die Grundsätze und die daraus abgeleiteten Anforderungen können nur dann gewahrt werden, wenn diese Annahmen stimmen. Sind sie dagegen nicht realistisch, ist die Einhaltung der Grundsätze höchstwahrscheinlich gefährdet und/oder es kommt zu einem Verstoß gegen die Grundsätze.

Neben der Feststellung der allgemeinen anwendbaren Rechtsgrundsätze ist es daher wichtig, ein Mindestmaß für deren Einhaltung festzulegen. Darüber hinaus sollten die Annahmen im Rahmen der regelmäßigen Risikobewertung (s. Leitlinie 9) analysiert und sollte den Sicherheitsbelangen dabei genügend Raum gegeben werden.

Die detaillierten rechtlichen und technischen Anforderungen an IKT-Lösungen sollten von den festgelegten Rechtsgrundsätzen abgeleitet werden. Auch muss das jeweilige Mindestmaß ihrer Einhaltung festgelegt werden. Die technischen Anforderungen sollten funktionale und nicht funktionale Anforderungen (z.B. Anforderungen betreffend Pflege und Interoperabilität neben denen hinsichtlich Sicherheit, Gebrauchstauglichkeit und Barrierefreiheit) wie auch Annahmen umfassen. Bei den technischen Anforderungen sollte angegeben werden, welche Annahmen brauchbar sind und welche nicht (üblicherweise, weil sie nicht realistisch sind). Die Festlegung der Mindestmaße sollte auch eine Reihe von Annahmen umfassen. Die technischen Anforderungen und Annahmen sollten technologieneutral formuliert werden.

Der Entwicklungs- und Entscheidungsprozess für das Ableiten der technischen Anforderungen – einschließlich der Mindestmaße und der brauchbaren Annahmen – sollte dokumentiert werden, Informationen über die beteiligten Personen enthalten (möglichst ein interdisziplinäres Team) und öffentlich zugänglich gemacht werden, um somit ein transparentes Verfahren sicherzustellen.

Die Regelungen sollten auf die Möglichkeiten der Klage und Streitbeilegungsverfahren in Bezug auf den Einsatz von IKT-Lösungen hinweisen und darauf eingehen, wie mit möglichen Beschwerden über Unregelmäßigkeiten umgegangen wird.

2. Die Mitgliedstaaten sollten durch Anwendung eines menschenzentrierten Ansatzes die Gebrauchstauglichkeit und Barrierefreiheit von bei Wahlprozessen eingesetzten IKT-Lösungen gewährleisten.

Kriterien für die Gebrauchstauglichkeit von IKT-Lösungen werden beispielsweise in der ISO-Norm 9241 definiert.[2] Die für größere Gruppen von Menschen, insbesondere Wähler, gedachten Benutzeroberflächen sollten nach strengeren Kriterien konzipiert werden als die für kleinere Gruppen von Fachanwendern wie Wahlhelfern. Bei den Anforderungen an die Barrierefreiheit sollten die Bedürfnisse der Nutzer berücksichtigt werden und es sollte sichergestellt werden, dass IKT-Lösungen allen – ob mit oder ohne Behinderung – zugänglich sind. Gebrauchstauglichkeit und Barrierefreiheit ergänzen sich somit gegenseitig. Die rechtlichen und technischen Anforderungen an die Gebrauchstauglichkeit und die Barrierefreiheit und das erforderliche Mindestmaß ihrer Erfüllung sollten gemäß Leitlinie 1 definiert werden. Diese zweite Leitlinie behandelt den Entwicklungsprozess.

[2] www.iso.org/standard/52075.html.

Bei der Entwicklung von IKT-Lösungen für Wahlprozesse sollte ein menschenzentrierter Ansatz gewählt werden. Das bedeutet, dass (künftige) Nutzer von IKT-Lösungen von Anfang an in den Entwicklungs- und Konzeptionsprozess eingebunden werden sollten. Dies kann über halbstrukturierte Befragungen und Fokusgruppen erfolgen, über die Möglichkeit, Rückmeldungen (auf Papier) zu Prototypen und Prozessen zu geben, und über Nutzerstudien. Ein menschenzentrierter Ansatz beinhaltet auch die Durchführung von Umfragen, nachdem IKT-Lösungen bei Wahlprozessen eingesetzt wurden, um Rückmeldungen aus der Praxis zur langfristigen Verbesserung der Gebrauchstauglichkeit und Barrierefreiheit einzuholen.

3. Wenn Mitgliedstaaten sich für eine nicht allgemein zugängliche elektronische Lösung entscheiden, sollte auch eine alternative, weithin zugängliche Lösung angeboten werden.

Das universelle Wahlrecht bedeutet, dass alle an den Wahlen Beteiligten alle Aufgaben erledigen und alle Rechte ausüben können, die das Gesetz für sie vorsieht. In Fällen, in denen die IKT-Lösung nicht allgemein zugänglich ist, kann ein paralleles, gleichwertiges Verfahren, das für die meisten Nutzer zugänglich ist, erforderlich sein. Es sollte auch angemerkt werden, dass in einigen Fällen der Einsatz von IKT für einige Menschen mehr Zugang schafft als die herkömmlichen Lösungen in Papierform.

Durch das Beibehalten eines alternativen Verfahrens neben dem Einsatz von IKT stellen die Mitgliedstaaten sicher, dass alle Beteiligten, denen das allgemeine Wahlrecht zusteht, Zugang haben und dass keine digitale Kluft entsteht bzw. diese sich nicht vergrößert. Das setzt voraus, dass Nutzerkreise ermittelt werden, die Barrierefreiheit bewertet und eine alternative und weithin zugängliche Lösung entwickelt und beibehalten wird. Die Öffentlichkeit sollte über die alternative Lösung informiert werden.

In den Regelungen sollte der rechtliche Wert der Ergebnisse von parallel bestehenden alternativen Lösungen sowie die Frage geklärt werden, welche Regeln anzuwenden sind, wenn diese Lösungen von ein und derselben Person genutzt werden. Die Regelungen sollten darüber hinaus auch bestimmen, wie mit Konflikten und anderen potenziellen Problemen umgegangen wird, welche durch die Nutzung mehrerer Kanäle für denselben Prozess entstehen.

4. Die Mitgliedstaaten sollten die Integrität und Authentizität von Informationen gewährleisten, die über die im Rahmen eines Wahlprozesses eingesetzten IKT-Lösungen geliefert werden. Es sollten Verfahren eingerichtet werden, mit denen Fehler oder ein unbefugter Eingriff aufgedeckt und wenn möglich korrigiert werden.

IKT-Lösungen sollten Authentifizierungsmechanismen vorsehen, um unbefugte Änderungen entsprechend den in der Leitlinie 1 aufgeführten Annahmen zu verhindern. IKT-Lösungen für Wahlprozesse sollten ohne Fehler oder unbefugte Änderungen funktionieren und so zur Integrität der Wahlen beitragen. Bei der Organisation von Wahlen sollte eine genaue gegenseitige Kontrolle in allen wichtigen Wahlphasen vorgesehen werden. Eine solche Überprüfung der Integrität ist wesentlicher Bestandteil der Maßnahmen zur allgemeinen Sicherheit und Cybersicherheit, um die Wahlen vor externen Angriffen und/oder unbefugtem internen Zugriff zu schützen, und der Maßnahmen zum Umgang mit möglichen Fehlbedienungen oder Fehlern in der Software oder Hardware. Es sollten Protokolle eingerichtet werden, um solche Vorfälle aufzudecken und effektiv auf sie zu reagieren. Für die Durchführung der Prüfungen sollte ein geeignetes Maß an Unabhängigkeit vorgesehen werden.

Idealerweise sollten unbefugte Änderungen oder Fehler im elektronischen Prozess oder Dokument entdeckt und korrigiert werden. Ist dies nicht möglich, sollten entsprechende Annahmen gemäß Leitlinie 1 formuliert werden. Es ist wichtig, dass in allen Phasen des Wahlprozesses Fehler oder Manipulationen aufgedeckt und korrigiert werden können, einschließlich bei der Bearbeitung von Wählerverzeichnissen wie auch bei der Auszählung und Übermittlung von Ergebnissen aus Wahllokalen an eine regionale oder zentrale Behörde, insbesondere wenn die Übermittlung über das Internet erfolgt.

Vorzugsweise sollte jemand im Fall unbefugter Änderungen oder von Fehlern zur Rechenschaft gezogen werden können. Es ist äußerst wichtig, dass ein nachvollziehbares und transparentes Verfahren für die Interaktion mit einem laufenden System, das Korrigieren von Daten oder das Wechseln bzw. Ersetzen eines fehlerhaften Systems vorgesehen wird. Die Interaktion mit einem laufenden System zu diesen Zwecken sollte im Rahmen der Risikoanalysen (s. Leitlinien 1 und 9) behandelt werden.

Die Beteiligten sollten überprüfen können, ob die Auszählung und Übermittlung der Ergebnisse korrekt durchgeführt wurde. Dies ist unter anderem möglich durch den Einsatz statistischer Überprüfungen numerischer Wahlergebnisse wie beispielsweise risikobegrenzende Audits und verschiedene Arten von Beobachtungen auf der Grundlage länderspezifischer Fachkompetenz.

5. Die Mitgliedstaaten sollten die Verfügbarkeit und Verlässlichkeit der im Wahlprozess eingesetzten IKT-Lösungen gewährleisten.

IKT-Lösungen sollten verfügbar und verlässlich sein. Eine IKT-Lösung sollte entsprechend den Anforderungen und Annahmen funktionieren, auch im Fall eines Systemausfalls oder von Fehlern durch Nutzer oder anderen Personen oder im Fall von Angriffen. Darüber hinaus sollte eine IKT-Lösung

verlässlich sein. Ihre Funktionalität sollte erhalten bleiben, auch wenn es in anderen Teilen des Wahlprozesses in der Hardware oder Software zu Mängeln kommt. Alternativ sollten Maßnahmen vorgesehen sein, um Informationen über vorab eingerichtete Ersatzlösungen und -kanäle bereitzustellen und diese zu aktivieren, einschließlich Lösungen, die keine aktive Verbindung erfordern.

Es sollten Pläne für die Reaktion auf Vorfälle und die Aufrechterhaltung des Betriebs eingerichtet und regelmäßig getestet werden. Sicherheitsmaßnahmen zur Gewährleistung der Verfügbarkeit und Zuverlässigkeit umfassen – unter anderem und ohne dass die folgende Aufzählung abschließend wäre – die Verwaltung von Zugriffsrechten für das System, Verfahren für Systemtests im Vorfeld der Wahlen, Verfahren für die Durchführung von Aktualisierungen im laufenden Betrieb, Sicherheitsregeln für die Übermittlung von Informationen außerhalb eines geschützten Umfelds, Datenschutzbestimmungen, die Erkennung von Unregelmäßigkeiten durch das System und Kommunikation bei auftretenden Problemen. Dies kann Verfahren gemäß ISO-Normen wie beispielsweise der ISO 27000-Reihe umfassen.

6. Die Mitgliedstaaten sollten entsprechend den Anforderungen der Wahl- und Datenschutzgesetze die Geheimhaltung und Vertraulichkeit von in IKT-Lösungen gespeicherten Informationen gewährleisten.

Die Erfüllung der aus den einschlägigen Rechtsgrundsätzen abgeleiteten Anforderungen an die Geheimhaltung und Vertraulichkeit sollten – auch unter Berücksichtigung der ebenfalls zu treffenden Annahmen – wie in Leitlinie 1 dargelegt sichergestellt sein. Dies umfasst auch Überlegungen zur langfristigen Geheimhaltung, d.h. ob die Geheimhaltung im weiteren Zeitverlauf gewährleistet werden soll oder nicht (da heutzutage verschlüsselte Daten gespeichert werden können, die zu einem späteren Zeitpunkt mit bestehenden oder neuen Lösungen wie Quantencomputern, zu denen es vermutlich einen breiteren Zugang geben wird, entschlüsselt werden könnten).

Datenschutzgrundsätze wie Privacy by Design oder Datenminimierung sind Mindestanforderungen und sollten bei jedem Einsatz von IKT im Wahlprozess bedacht werden. Für jede spezifische eingesetzte IKT-Lösung sollten die Mitgliedstaaten darüber hinaus überlegen, ob zusätzlich geeignete, spezifische und über die Datenschutzmaßnahmen hinausgehende Maßnahmen erforderlich sind, um die Grundrechte der betroffenen Person gemäß beispielsweise Artikel 6 Absatz 1 des Übereinkommens des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (ETS Nr. 108) sicherzustellen. Stellt ein Mitgliedstaat einen Bedarf an solchen spezifischen Maßnahmen fest, sollten diese Teil der Wahlordnung werden.

Konflikte zwischen Transparenz einerseits und Vertraulichkeit und Geheimhaltung andererseits sollten sorgfältig berücksichtigt werden (s.a. Leitlinie 7).

7. Die Mitgliedstaaten sollten die Transparenz der Wahl sowie der dabei eingesetzten IKT-Lösungen gewährleisten.

Transparenz in jeglicher Hinsicht ist bei einer Wahl von entscheidender Bedeutung, um eine erfolgreiche und vertrauenswürdige Wahl durchzuführen und das Vertrauen in den Wahlprozess zu stärken. Dies gilt umso mehr, wenn dabei IKT-Lösungen zum Einsatz kommen. Für IT-Laien gestaltet es sich zunehmend schwierig, IKT-Lösungen zu verstehen. Daher muss die Fähigkeit aller Beteiligten, die IKT-Lösungen zu verstehen, erhöht werden.

Alle relevanten Beteiligten sollten über den Einsatz von IKT-Lösungen einschließlich über deren Einführung in den Wahlprozess, ihren Betrieb und die Bewertung des Einsatzes der Lösung nach der Wahl informiert werden. Die Informationen zu ihrer Einführung sollten Folgendes beinhalten:

1. eine Erläuterung der Gesamtstrategie;
2. die Veröffentlichung der technischen Anforderungen, der getroffenen Annahmen und von Informationen dazu, wie die Anforderungen erfüllt werden sollten;
3. die Benennung von bei früheren Wahlen festgestellten Defiziten;
4. Details zum Entwicklungs- und Entscheidungsprozess, unter anderem auch über die gesammelten Beiträge und das beteiligte (interdisziplinäre) Team;
5. Informationen zur Realisierbarkeit der Gesamtumsetzung;
6. Informationen über die Beschaffung der Lösung und die diesbezügliche Organisation;
7. Informationen zur umfassenden Evaluierung vor Beginn des Einsatzes der IKT-Lösung sowie Informationen über die Ergebnisse der kontinuierlichen Risikobewertung;
8. Informationen dazu, wie mit widersprüchlichen oder konkurrierenden Grundsätzen wie etwa Privatsphäre und Geheimhaltung versus Transparenz umzugehen ist;
9. die Veröffentlichung des Quellcodes.

Zur Transparenz gehört es auch, Beobachtern Zugang zur Dokumentation und zu den Prozessen zu ermöglichen, idealerweise in einer ihnen vertrauten Sprache.

Darüber hinaus sollten Transparenzmaßnahmen auch Bestimmungen für strukturierte (maschinenlesbare) Daten zum Wahlprozess (wie etwa zu den Standorten der Wahllokale und ihren Öffnungszeiten, Kandidatenlisten und Wahlergebnissen) beinhalten, und zwar auch als Open Data.

Die Transparenzanforderungen sollten darauf abzielen, eine genaue Prüfung durch die Öffentlichkeit zu ermöglichen. Es sollten geeignete Prozesse eingerichtet werden, um Rückmeldungen aus der Öffentlichkeit entgegenzunehmen, zu beantworten und zu diskutieren und die entsprechenden Schlussfolgerungen zu verarbeiten. Transparenz kann damit dazu beitragen, die Gesamtsicherheit des Wahlprozesses und des Vertrauens in selbigen zu verbessern.

Schließlich ist Transparenz ein Querschnittsthema und berührt als solches auch andere Leitlinien. Sie erfordert unter anderem die Veröffentlichung von Annahmen (Leitlinie 1); die Bereitstellung von Informationen über den Entwicklungs- und Entscheidungsprozess zur Aufstellung der Gebrauchstauglichkeits- und Barrierefreiheitskriterien (Leitlinie 2); die Organisation eines transparenten Verfahrens für die Interaktion mit einem laufenden System, die Korrektur von Daten oder den Wechsel oder das Ersetzen eines fehlerhaften Systems (Leitlinie 4); die Dokumentation von Entscheidungen zur Verfügbarkeit und Zuverlässigkeit einschließlich der jeweiligen Anforderungen (Leitlinie 5); die Dokumentation von Entscheidungen zur Sicherheit und Vertraulichkeit einschließlich Entscheidungen über deren Abstimmung auf die Transparenzanforderungen (Leitlinie 6); die Dokumentation der Anforderungen für die Systemevaluierung (Leitlinie 8) oder die Dokumentation des Risikomanagement-Prozesses (Leitlinie 9).

8. Die Mitgliedstaaten sollten vor der Implementierung eine von unabhängigen Experten durchgeführte Evaluierung der im Wahlprozess eingesetzten IKT-Lösungen organisieren.

Diese Leitlinie befasst sich mit dem Evaluierungsprozess vor der Implementierung einer IKT-Lösung im Wahlprozess. Die Evaluierung sollte sich auf Sicherheits-, Gebrauchstauglichkeits- und Barrierefreiheitsaspekte erstrecken, jedoch nicht darauf beschränkt sein. Es sollten die gesamte IKT-Lösung und ihre Nutzungsumgebung betrachtet werden.

Die Evaluierungsansätze einschließlich der Prüftiefe sollten festgelegt werden. Idealerweise sollte ein standardisierter Evaluierungsansatz bevorzugt werden. Als Voraussetzung sollte das Evaluierungsziel klar definiert werden.

Für die Evaluierung sind mehrere Dokumente erforderlich, die im Falle einer standardisierten Evaluierung eindeutig festgelegt müssen. Es sollte – bereits zu einem sehr frühen Zeitpunkt – festgelegt werden, ob die Evaluierung nur von ausgewählten Experten mit Zugang zur IKT-Lösung, dem Quellcode und der Dokumentation durchgeführt werden soll und/oder ob eine Bewertung (oder Teile davon) von jedermann durchgeführt werden kann, weil die IKT-Lösung, der Quellcode und die Dokumentation öffentlich zugänglich sind.

Auch sollte festgelegt werden, wie die Unabhängigkeit der Evaluierung erreicht werden soll. Die Experten sollten so unabhängig wie möglich sein. Dies kann erzielt werden, indem zwei Stellen eingebunden werden: Eine hat den Auftrag, die eigentliche Evaluierung durchzuführen, während die andere – eine staatliche Organisation – die evaluierende Stelle überwacht. Möglicherweise werden für verschiedene Anforderungsbereiche (wie etwa Sicherheit oder Gebrauchstauglichkeit/Barrierefreiheit) unterschiedliche Experten benötigt. Schließlich ist es wichtig, zu berücksichtigen, wie viel Zeit die unabhängigen Experten für die Evaluierung benötigen.

Die Evaluierungsanforderungen und der Evaluierungsansatz sowie die Evaluierungsergebnisse und Informationen zu den daran beteiligten Stellen/Personen (möglichst ein interdisziplinäres Team) sollten öffentlich zugänglich gemacht werden.

9. Die Mitgliedstaaten sollten ein kontinuierliches Risikomanagement für die im Wahlprozess eingesetzten IKT-Lösungen durchführen.

Prozesse, die für den korrekten Ablauf einer Wahl und die Ermittlung richtiger Ergebnisse wichtig sind, können mit ähnlichen Risiken wie e-Voting verbunden sein, insbesondere wenn die zugrunde liegende Lösung webbasiert ist. Diese Risiken sollten Gegenstand eines entsprechenden Risikomanagements sein. Besonders bei ermittelten Sicherheitsrisiken sollten angemessene Gegenmaßnahmen entwickelt werden.

Die Risiken sollten aus den Anforderungen und Annahmen (Leitlinie 1) und dem Evaluierungsergebnis (Leitlinie 8) abgeleitet werden. Das Risikomanagement ist somit im Entwicklungsprozess und während der Nutzung der IKT-Lösung im Wahlprozess sowie in der Vorbereitung künftiger Wahlen von Bedeutung. Die Evaluierung der aktuellen Risiken und die Entscheidung darüber, ob verbleibende Risiken weiterhin akzeptabel sind, sind ein kontinuierlicher Prozess. Dies ist insofern besonders wichtig, als im Laufe der Zeit neue Angriffsarten zum Einsatz kommen.

Es ist wichtig, sich der verbleibenden Risiken bewusst zu sein. Außerdem sollte entschieden werden, ob und wie mit diesen Risiken umgegangen werden soll. Die Risikomanagement-Ansätze sollten Notfallpläne einschließen.

Mit Blick auf das Risikomanagement sollte entschieden werden, welche Informationen öffentlich zugänglich gemacht werden sollten und welche nicht, wobei beachtet werden sollte, dass „Sicherheit durch Intransparenz“ im Allgemeinen als kontraproduktiv angesehen wird.

Der Risikomanagement-Ansatz sollte regelmäßig und mindestens nach jeder Wahl erneut geprüft werden. Etwaige ungewöhnliche Fälle, Probleme oder Beschwerden sollten berücksichtigt werden.

Der Risikomanagement-Ansatz sowie die Informationen zu den daran beteiligten Stellen/Personen (möglichst ein interdisziplinäres Team) sollten öffentlich zugänglich gemacht werden.

10. Die Mitgliedstaaten sollten die erforderlichen Kapazitäten aufbauen und vorhalten, um den Einsatz von IKT-Lösungen im Wahlprozess zu beurteilen, einzuführen und zu managen.

Bei der Einführung von IKT in eine beliebige Phase des Wahlzyklus ist es wesentlich, dass die Mitgliedstaaten über die erforderliche administrative und technische Kapazität und die damit im Zusammenhang stehenden Ressourcen einschließlich Finanzmitteln verfügen, um die Technologie erfolgreich und nachhaltig zu planen, zu implementieren und zu betreiben.

Die Mitgliedstaaten sollten unter anderem den Automatisierungsgrad des gesamten Wahlprozesses und mögliche Synergien zwischen der neuen Lösung und bestehenden Low- oder Hightech-Lösungen berücksichtigen. Idealerweise sollten sie eine umfassendere Strategie für bestehende IKT-bezogene Investitionen haben.

Von wesentlicher Bedeutung für die administrative und technische Kapazität sind qualifizierte Arbeitskräfte, die kontinuierlich geschult und mit den erforderlichen Tools und Mitteln ausgestattet werden sollten und denen vor allem ausreichend Zeit eingeräumt werden sollte, sich auf ihre Aufgaben zu konzentrieren.

Grundsätzliches Ziel bei der Vorhaltung dieser erforderlichen Kapazitäten ist es, zu vermeiden, dass wesentliche administrative Wahlaufgaben an gewinnorientierte Dritte ausgelagert werden müssen, und so die relevanten Behörden zu befähigen, die Wahl gemäß den gesetzlichen Anforderungen zu überwachen, ohne von privaten Dritten abhängig zu sein.

11. Die Mitgliedstaaten sollten grundsätzlich verantwortlich sein, auch wenn private Akteure beteiligt sind.

Bei der Organisation von Wahlen liegt die grundsätzliche Verantwortung für die korrekte Umsetzung und Durchführung des Wahlprozesses beim jeweiligen Mitgliedstaat. Dies ist auch dann der Fall, wenn Dritte (einschließlich privater Akteure) den Mitgliedstaat bei der Durchführung des Wahlprozesses unterstützen oder wenn Teile des Wahlprozesses an Dritte ausgelagert und/oder vergeben werden. Dritte müssen dieselben Normen und Erwartungen beachten und erfüllen wie die Mitgliedstaaten. Entsprechende Bestimmungen sollten in die vertraglichen Vereinbarungen aufgenommen werden.

12. Die Mitgliedstaaten sollten sich proaktiv mit dem möglichen Einsatz von IKT-Lösungen in Situationen auseinandersetzen, in denen höhere Gewalt sich auf die reguläre Durchführung von Wahlen auswirkt.

In jüngster Vergangenheit haben die bei der Anpassung der Wahlverfahren an die neuen, pandemiebedingten Umstände gesammelten Erfahrungen die Frage der Einführung von IKT-Lösungen als Unterstützung im Umgang mit solchen außergewöhnlichen Umständen ins Licht gerückt. Wie diese Leitlinien jedoch zeigen, kann der Einsatz von IKT-Lösungen nicht als kurzfristige Abhilfe für außergewöhnliche Lagen betrachtet werden. Stattdessen sollte er Teil einer längerfristigen Planung des Wahlprozesses und eines umfassenderen Ansatzes für den Umgang mit außergewöhnlichen Ereignissen sein.

Die Mitgliedstaaten sollten sich proaktiv mit künftigen Störereignissen wie Pandemien auseinandersetzen. Wenn Mitgliedstaaten beabsichtigen, IKT-Lösungen unter solchen außergewöhnlichen Umständen einzusetzen, so wird ihnen geraten, sich entsprechend den oben dargelegten Leitlinien vorab auf solche Eventualitäten vorzubereiten.

Glossary of some terms used in the guidelines

- **Accessibility:** accessibility is about designing products and systems that are accessible for everyone, whether a person has a disability or not. At the same time, accessibility may specifically address discriminatory aspects related to equivalent user experiences, focusing on people with disabilities to ensure inclusion.[3]
- **Assumption**: Assumptions describe conditions that the operational environment in which the ICT solution is used needs to meet, if it is to provide all of its security functionality. "If the Target of evaluation (TOE) [the ICT solution] is placed in an operational environment that does not meet these assumptions, the TOE may not be able to provide all of its security functionality anymore. Assumptions can be on physical, personnel and connectivity of the operational environment."[4] The Guidelines recommend transparency about the assumptions and their evaluation (see Guidelines 1 and 7). Their "realistic/unrealistic" status should be periodically re-evaluated (see Guideline 9 on risks management policy).
- **Authenticity (of the information)**: the property that data originated from its purported source.[5]
- **Availability**: ensuring timely and reliable access to and use of information and systems.[6]
- **Elections**: political election or referendum.
- **Human-centred (design)**: (as used in ISO standards) is an approach to problem solving, commonly used in design and management frameworks, that develops solutions to problems by involving the human perspective in all steps of the problem-solving process. Human involvement typically takes place in observing the problem within context, brainstorming, conceptualising, developing and implementing the solution.[7]
- **ICT**: information and communication technology. In these guidelines, it equates to products and processes that store, retrieve, manipulate, transmit or receive information electronically in a digital form.
- **Integrity (of the information)**: the property that data have not been altered in an unauthorised manner. Data integrity covers data in storage, during processing and while in transit.[8]
- **Member State**: in these guidelines, "member State" refers to the authority in charge of regulating, conducting, or supervising the electoral process in question. Usually, but not always, it refers to the electoral management body at local, regional, or central level. It may also refer to other public institutions such as the parliament or the government.
- **Minimum level (to which legal principles should be ensured)**: it is often not possible to ensure the full respect of all principles because there might be conflicting or competing principles, such as secrecy and data protection on one side and transparency on the other. In these cases, a balance of interest must be reached and the minimum level, to which each of the conflicting principles should be ensured, needs to be defined. This decision should be taken by the competent authority, usually the legislator. The essence of the principles cannot be violated.
- **Reliability**: the ability of a system or component to function under stated conditions for a specified period of time.[9]
- **(Technical) Requirement**: a condition or capability that must be met or possessed by a system or system element to satisfy a contract, standard, specification or other formally imposed documents.[10]
- **(Legal) Requirement**: a legal requirement is a concretisation of a legal principle. For instance, the legal requirements that apply to the transmission of results from polling stations to a central election commission (for example, requirements for deadlines, formats or checks) are derived from and are a concretisation of the principles of universal, equal, free and secret suffrage.
- **Risk**: the level of impact on organisational operations (including mission, functions, image, or reputation), organisational assets or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.[11]
- **Threat:** Any circumstance or event with the potential to harm an electoral ICT system through unauthorised access, destruction, disclosure, modification of data, and/or denial of service.
- **Usability**: usability is about designing products to be effective, efficient, and satisfying. It includes user experience design and is closely related to accessibility.[12]

---

[3]. Definition taken from: www.w3.org/WAI/fundamentals/accessibility-usability-inclusion/.
[4]. Definition taken from: https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf
[5]. Definition taken from: https://csrc.nist.gov/glossary/term/authenticity.
[6]. Definition taken from: https://csrc.nist.gov/glossary/term/availability.
[7]. Definition taken from: www.w3.org/WAI/redesign/ucd.
[8]. Definition taken from: https://csrc.nist.gov/glossary/term/data_integrity.
[9]. Definition taken from: https://csrc.nist.gov/glossary/term/reliability.
[10]. Definition taken from: https://csrc.nist.gov/glossary/term/requirement.
[11]. Definition taken from: https://csrc.nist.gov/glossary/term/risk.
[12]. Definition taken from: www.w3.org/WAI/fundamentals/accessibility-usability-inclusion/.