b) forhindre, at personer uden bemyndigelse får adgang til nationale anlæg, hvor medlems staten udfører operationer i overensstemmelse med formålene med VIS (kontrol ved indgangen til anlægget)
c) forhindre, at databærere kan læses, kopieres, ændres eller fjernes af personer uden bemyndigelse (kontrol med databærere)
d) forhindre uautoriseret indlæsning af oplysninger samt uautoriseret læsning, ændring eller sletning af indlæste personoplysninger (kontrol med opbevaring)
e) forhindre uautoriseret behandling af oplysninger i VIS samt uautoriseret ændring eller sletning af oplysninger, som er blevet behandlet i VIS (kontrol med indlæsning af oplysninger)
f) sikre, at bemyndigede personer kun får adgang til de oplysninger i VIS, som hører ind under deres bemyndigelse, og kun ved hjælp af individuelle og entydige brugeridentiteter og fortrolige adgangsmetoder (kontrol med dataadgang)
g) sikre, at alle myndigheder med adgangsret til VIS opretter profiler, der beskriver funktioner og ansvarsområder for de personer, som er bemyndiget til at få adgang til, indlæse, ajourføre, slette og søge i oplysningerne, og på anmodning straks stiller disse profiler til rådighed for de nationale tilsynsmyndigheder, der er omhandlet i ar-tikel 41 (personaleprofiler)
h) sikre, at det er muligt at efterprøve og fastslå, hvilke myndigheder personoplysninger må videregives til via datatransmissionsudstyr (kontrol med videregivelse)
i) sikre, at det er muligt at efterprøve og fastslå, hvilke oplysninger der er blevet behandlet i VIS, hvornår, af hvem og til hvilket formål (kontrol med registrering af oplysninger)
j) forhindre uautoriseret læsning, kopiering, ændring eller sletning af personoplysninger under fremsendelsen af personoplysninger til eller fra VIS eller under fremsendelsen af databærere, navnlig ved hjælp af passende krypteringsteknikker (kontrol med transport)
k) overvåge effektiviteten af de sikkerhedsforanstaltninger, der er omhandlet i dette stykke, og træffe de nødvendige organisatoriske foranstaltninger vedrørende intern kontrol for at sikre overholdelsen af denne forordning (egenkontrol).

3. Forvaltningsmyndigheden træffer de nødvendige foranstaltninger med henblik på at opfylde målsætningerne i stk. 2 for så vidt angår driften af VIS, herunder vedtagelsen af en sikkerhedsplan.

Artikel 33

Erstatningsansvar

1. Enhver person eller medlems stat, som har lidt skade som følge af en ulovlig behandling eller enhver anden handling, der er i strid med denne forordning, har ret til erstatning fra den medlemsstat, som er ansvarlig for skaden. Den pågældende medlemsstat fritages helt eller delvis for erstatningsansvar, hvis den kan bevise, at den ikke er skyld i den begivenhed, der medførte skaden.

2. Hvis en medlemsstats manglende overholdelse af sine forpligtelser i henhold til denne forordning volder skade på VIS, holdes den pågældende medlems stat ansvarlig for skaden, medmindre Forvaltningsmyndigheden eller en anden af de medlems stater, der deltager i VIS, ikke har truffet rimelige foranstaltninger til at forhindre skaden i at ske eller til at begrænse dens omfang.

3. Skadeserstatningskrav mod en medlemsstat, der fremsættes efter stk. 1 og 2, behandles efter den sagsøgte medlemsstats nationale ret.

Artikel 34

Føring af registre

1. Hver medlems stat og Forvaltningsmyndigheden fører registre over alle behandlinger af oplysninger i VIS. Disse registre skal vise formålet med adgangen, jf. artikel 6, stk. 1, og artikel 15-22, datoen og tidspunktet, den type oplysninger, der er fremsendt, jf. artikel 9-14, den type oplysninger, der er anvendt til søgningen, jf. artikel 15, stk. 2, artikel 17, artikel 18, stk. 1-3, artikel 19, stk. 1, artikel 20, stk. 1, artikel 21, stk. 1, og artikel 22, stk. 1, og navnet på den myndighed, der har indlæst eller hentet oplysningerne. Desuden fører hver medlemsstat registre over de personer, som er ansvarlige for at indlæse eller hente oplysningerne.